Symantec NetBackup™ Cloud Administrator's Guide

UNIX, Windows, Linux

Release 7.6

Symantec NetBackup™ Cloud Administrator's Guide

Documentation version: 7.6

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

About NetBackup Cloud storage

This chapter includes the following topics:

About cloud storage features and functionality

NetBackup Cloud Storage enables you to back up and restore data from cloud Storage as a Service (STaaS) vendors. NetBackup Cloud Storage is integrated with Symantec OpenStorage.

Table 1-1 outlines the features and functionality NetBackup Cloud Storage delivers.

Table 1-1 Features and functionality

Feature	Details
Configuration Wizard	A Cloud Storage Server Configuration Wizard is incorporated to facilitate the cloud storage setup and storage provisioning. Cloud storage provisioning now happens entirely through the NetBackup interface.
Encryption	NetBackup Cloud Storage Encryption encrypts the data inline before it is sent to the cloud. Encryption interfaces with the NetBackup Key Management Service (KMS) to leverage its ability to manage encryption keys. The encryption feature uses an AES 256 cipher feedback (CFB) mode encryption.

Table 1-1 Features and functionality *(continued)*

Feature	Details
Throttling	NetBackup Cloud Storage throttling controls the data transfer rates between your network and the cloud. The throttling values are set on a per NetBackup media server basis. In certain implementations, you want to limit WAN usage for backups and restores to the cloud. You want to implement this limit so you do not constrain other network activity. Throttling provides a mechanism to the NetBackup administrators to limit NetBackup Cloud Storage traffic. By implementing a limit to cloud WAN traffic, it cannot consume more than the allocated bandwidth. NetBackup Cloud Storage Throttling lets you configure and control the following: ■ Different bandwidth value for both read and write operations. ■ Maximum number of connections that are supported for each cloud provider at any given time. ■ Network bandwidth as a percent of total bandwidth. ■ Network bandwidth per block of time.
Metering	The NetBackup Cloud Storage metering reports enable you to monitor data transfers within NetBackup Cloud Storage. Cloud-based storage is unlike traditional tape or disk media, which use persistent backup images. Your cloud storage vendor calculates cloud-based storage costs per byte stored and per byte transferred. The NetBackup Cloud Storage software uses several techniques to minimize stored and transferred data. With these techniques, traditional catalog-based information about the amount of protected data no longer equates to the amount of data that is stored or transferred. Metering allows installations to monitor the amount of data that is transferred on a per media server basis across one or more cloud-based storage providers. Metering reports are generated through NetBackup OpsCenter.
Cloud Storage service	The NetBackup CloudStore Service Container (`nbcssc`) process performs the following functions: ■ Controls the configuration parameters that are related to NetBackup Cloud Storage ■ Generates the metering information for the metering plug-in ■ Controls the network bandwidth usage with the help of throttling plug-in On Windows, it is a standard service installed by NetBackup. On UNIX, it runs as a standard daemon.

Table 1-1 Features and functionality *(continued)*

Feature	Details
Storage providers	Symantec currently supports several cloud storage providers. More information is available about each of these vendors. See "About the Amazon Simple Storage Service (S3) requirements" on page 17. See "About AT&T Synaptic requirements" on page 19. See "About Rackspace Cloud Files requirements" on page 20.
OpsCenter Reporting	Monitoring and reporting of the data that is sent to cloud storage is available through new cloud reports in OpsCenter. The cloud reports include: ■ **Job Success Rate**: Success rate by backup job level across domains, clients, policies, and business level views filtered on cloud-based storage. ■ **Data Expiring In Future**: Data that expires each day for the next seven days filtered on cloud-based storage. ■ **Cloud Metering**: Historical view of the data that is written to cloud per cloud provider. ■ **Average Data Transfer Rate**: Historical view of average data transfer rate to cloud per cloud provider. ■ **Cloud Metering Chargeback**: Ranking, forecast, and distribution view of the cost that is incurred on cloud-based storage per cloud provider.

About unsupported OpenStorage capabilities

None of the cloud providers support the following OpenStorage capabilities:

- Optimized duplication
- Direct to tape (by NDMP)
- Disk volume spanning of backup images

Chapter 2

Configuring cloud storage in NetBackup

This chapter includes the following topics:

Configuring cloud storage in NetBackup

This topic describes how to configure cloud storage in NetBackup. Table 2-1 provides an overview of the tasks to configure cloud storage. Follow the steps in the table in sequential order.

The NetBackup administrator's guide describes how to configure a base NetBackup environment.

See the NetBackup Administrator's Guide, Volume I.

Table 2-1 Overview of the NetBackup cloud configuration process

Step	Task	More information
Step 1	Create NetBackup log file directories on the master server and the media servers	See "About NetBackup cloud storage log files" on page 90. See "Creating NetBackup log file directories" on page 89.
Step 2	Review the cloud installation requirements	See "Cloud installation requirements" on page 16.
Step 3	Determine the requirements for provisioning and configuring your cloud storage provider in NetBackup	See "About the cloud storage providers" on page 17.
Step 4	Understand the role of the Cloud Storage Service Container	See "About the NetBackup CloudStore Service Container" on page 27.
Step 5	Configure the global cloud storage host properties as necessary	See "Scalable Storage properties" on page 22.
Step 6	Understand key management for encryption	Encryption is optional. See "About key management for encryption of NetBackup cloud storage" on page 28.

Table 2-1 Overview of the NetBackup cloud configuration process *(continued)*

Step	Task	More information
Step 7	Configure key management manually	You can configure key management manually by using NetBackup commands. See "Configuring key management for NetBackup cloud storage encryption" on page 30. Alternatively, you can configure key management if you use NetBackup wizards: ■ The **Cloud Storage Server Configuration Wizard** lets you configure the key database key and the key record key. ■ The **Disk Pool Configuration Wizard** configures key groups and key names. **Note:** Regardless of how you configure key management, record your keys and store them in a safe place. See "Saving a record of the KMS key names for NetBackup cloud storage encryption" on page 34.
Step 8	Configure the storage server	See "About cloud storage servers" on page 36. See "Configuring a storage server for cloud storage" on page 37.
Step 9	Configure the disk pool	See "About cloud storage disk pools" on page 55. See "Configuring a disk pool for cloud storage" on page 56.
Step 10	Configure additional storage server properties	See "Cloud storage server properties" on page 46. See "Changing storage server properties in NetBackup" on page 65.
Step 11	Add additional media servers	Adding additional media servers is optional. See "About cloud storage data movers" on page 67. See "Adding backup media servers to your cloud environment" on page 67.
Step 12	Configure a storage unit	See "Configuring a storage unit for cloud storage" on page 68.

Table 2-1 Overview of the NetBackup cloud configuration process *(continued)*

Step	Task	More information
Step 13	Configure NetBackup Accelerator and optimized synthetic backups	Accelerator and optimzed synthetic backups are optional. See "About NetBackup Accelerator and NetBackup Optimized Synthetic backups" on page 72. See "Enabling NetBackup Accelerator with cloud storage" on page 73. See "Changing storage server properties in NetBackup" on page 65.
Step 14	Configure a backup policy	See "Creating a backup policy" on page 77.

Cloud installation requirements

When you develop a plan to implement a NetBackup Cloud solution, use Table 2-2 to assist with your plan.

Table 2-2 Cloud installation requirements

Requirement	Details
NetBackup media server platform support	NetBackup cloud storage is supported on the following operating systems for media servers: ■ AIX ■ HP-UX ■ RedHat Linux ■ Solaris 10 ■ SUSE Linux ■ Windows Server 2008 R2
Cloud storage provider account	You must have an account created with your preferred cloud storage provider before you configure NetBackup Cloud Storage. Please refer to the list of available NetBackup cloud storage providers. You can create this account in the Cloud Storage Configuration Wizard. See "About the cloud storage providers" on page 17.

Table 2-2 Cloud installation requirements *(continued)*

Requirement	Details
NetBackup cloud storage licensing	NetBackup cloud storage is enabled through the NetBackup Data Protection Optimization license key. To use NetBackup Accelerator with NetBackup cloud storage, you must install the Data Protection Optimization Option. that license key activates the NetBackup Accelerator feature.

About the cloud storage providers

The information that is required to configure cloud storage in NetBackup varies according to each cloud storage provider's requirements. Separate topics describe the requirements for each provider.

See "About the Amazon Simple Storage Service (S3) requirements" on page 17.

See "About AT&T Synaptic requirements" on page 19.

See "About Rackspace Cloud Files requirements" on page 20.

NetBackup supports private clouds from the supported cloud providers.

See "About private clouds from supported cloud vendors" on page 21.

About the Amazon Simple Storage Service (S3) requirements

NetBackup Cloud Storage enables Symantec NetBackup to back up data to and restore data from Amazon Simple Storage Service (S3).

Table 2-3 describes the details and requirements of Amazon Simple Storage Service.

Table 2-3 Amazon Simple Storage Service requirements

Requirement	Details
User account	You must obtain an Amazon Simple Storage Service (S3) account and the associated user name and password. You must also obtain an access ID and secure access token. These are required when you configure the storage server in NetBackup.

Table 2-3 Amazon Simple Storage Service requirements *(continued)*

Requirement	Details
Storage requirements	The following are the requirements for Amazon Simple Storage Service: ■ You must have a NetBackup Data Protection Optimization Option license key. ■ The bucket name must be between 3 and 255 characters. You can use the following characters for the bucket name: ■ Any of the 26 lowercase (small) letters of the International Standards Organization (ISO) Latin-script alphabet. These are the same lowercase (small) letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: . _ - (you cannot use any of these as the first character in the bucket name) ■ You can create a maximum of 100 buckets per Amazon account. You can delete empty buckets and then reuse the bucket name, but deleted buckets count toward the 100 bucket limit. ■ You must have an Amazon Simple Storage Service account user name and password. ■ Symantec recommends that you use NetBackup to create the buckets for your NetBackup backups. The Amazon S3 interface may allow characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential for problems. ■ NetBackup supports US Standard buckets only.
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

Note: The information that is displayed for **Used Capacity** and **Available Space** for Amazon is inaccurate in the NetBackup Administration Console. The values are found under **Media and Device Management > Devices > Disk Pool**. Even if there is information in the disk pool, the value that is displayed for **Used Capacity** is zero. The value for **Available Space** displays the maximum amount. You must review the information on the provider Web site for accurate use information.

NetBackup supports the private clouds from the supported cloud providers.

See “About private clouds from supported cloud vendors” on page 21.

More information about Amazon S3 is available from Amazon.

http://aws.amazon.com/s3/

About AT&T Synaptic requirements

NetBackup Cloud Storage enables Symantec NetBackup to back up data to and restore data from AT&T Synaptic™.

Table 2-4 describes the details and requirements of AT&T Synaptic.

Table 2-4 AT&T Synaptic requirements

Requirement	Details
User account	An AT&T Synaptic user ID and password are required to create the storage server.
Storage requirements	The following are the requirements for AT&T cloud storage: ■ You must have a NetBackup Data Protection Optimization Option license key. ■ You must use NetBackup to create the volume for your NetBackup backups. The volume that NetBackup creates contain a required Symantec Partner Key. If you use the AT&T Synaptic interface to create the volume, it does not contain the partner key. Consequently, that volume cannot accept data from NetBackup. ■ The logical storage unit (LSU) name (that is, volume name) must be 50 or fewer characters. You can use the following characters for the volume name: ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: `#$_-', ■ You must have an AT&T Synaptic account user name and password.

Note: The information that is displayed for **Used Capacity** and **Available Space** for AT&T is inaccurate in the NetBackup Administration Console. The values are found under **Media and Device Management > Devices > Disk Pool**. Even if there is information in the disk pool, the value that is displayed for **Used Capacity** is zero. The value for **Available Space** displays the maximum amount. You must review the information on the provider Web site for accurate use information.

NetBackup supports the private clouds from the supported cloud providers.

See “About private clouds from supported cloud vendors” on page 21.

More information about AT&T Synaptic is available from AT&T.

http://www.business.att.com/enterprise/Service/hosting-services/cloud/storage/

About Rackspace Cloud Files requirements

NetBackup Cloud Storage enables Symantec NetBackup to back up data to and restore data from Rackspace Cloud Files™.

Table 2-5 describes the details and requirements of Rackspace CloudFiles.

Table 2-5 Rackspace Cloud Files requirements

Requirement	Details
Rackspace Cloud Files accounts	You must obtain a Rackspace account. The account has a user name and password. You need to follow the Rackspace process to generate an access key. The user name and access key are required when you configure the storage server.
Storage requirements	The following are the requirements for Rackspace CloudFiles: ■ You must have a NetBackup Data Protection Optimization Option license key. ■ You must have a Rackspace Cloud Files account user name and password. ■ You must use NetBackup to create the cloud storage volume for your NetBackup backups. The volume that NetBackup creates contains a required Symantec Partner Key. If you use the Cloud Files interface to create the volume, it does not contain the partner key. Consequently, that volume cannot accept data from NetBackup. ■ You can use the following characters in the volume name: ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: `~!@#$%^&*()- _+=|\\[]{}':;?><.,

Note: The information that is displayed for **Used Capacity** and **Available Space** for Rackspace is inaccurate in the NetBackup Administration Console. The values are found under **Media and Device Management > Devices> Disk Pool**. Even if there is information in the disk pool, the value that is displayed for **Used Capacity** is zero. The value for **Available Space** displays the maximum amount. You must review the information on the provider Web site for accurate use information.

NetBackup supports the private clouds from the supported cloud providers.

See "About private clouds from supported cloud vendors" on page 21.

More information about Rackspace Cloud Files is available from Rackspace.

http://www.rackspace.com/cloud/cloud_hosting_products/files/

About private clouds from supported cloud vendors

NetBackup supports the private clouds from the supported cloud providers.

Note: NetBackup does not support both a private cloud and public cloud storage from the same vendor in the same NetBackup domain. Therefore, if you already have public or private cloud storage configured for a vendor, you cannot configure the other type.

Before you configure a private cloud in NetBackup, it must be set up and available.

Two methods exist to configure a private cloud storage server, as follow:

- Use the **Advanced Settings** dialog box
- Edit a cloud storage configuration file

See "Configuring a storage server for cloud storage" on page 37.

Use the Advanced Settings dialog box

On the select media server panel of the **Cloud Storage Configuration Wizard**, click the **Advanced Settings** button. Then, in the **Advanced Server Configuration** dialog box, select **Override storage server** and enter the name of the internal host to use as the storage server. Use the fully qualified host name or ensure that your network environment can resolve the name to an IP address.

The **Create an account with service provider** link on the wizard panel opens a cloud provider Web page in which you can create an account. If you configure a private cloud, that Web page has no value for your configuration process.

Edit a cloud storage configuration file

You can change a cloud storage configuration file to point at the internal host for your private cloud. If you do, the wizard automatically uses that host as the cloud storage server. You do not have to use the **Advanced Server Configuration** settings.

The following is the path name of the cloud storage configuration file:

- UNIX: `/usr/openv/java/cloudstorejava.conf`
- Windows: `C:\Program Files\Veritas\NetBackup\bin\cloudstorewin.conf`

The file has a section for each cloud provider. To specify the internal host for a vendor cloud type, change the value of the following parameter:

`DEFAULT_STORAGE_SERVER_NAME`

Use the fully qualified host name or ensure that your network environment can resolve the name to an IP address.

If you want the **Create an account with service provider** link on the wizard panel to open a different Web page, edit the following parameter in the configuration file:

`CLOUD_PROVIDER_URL`

If you edit this file while the **Cloud Storage Configuration Wizard** is open, you must exit from the wizard. Then, open it again so it can read the configuration file for the new settings.

Scalable Storage properties

The **Scalable Storage** properties contains the **Cloud Settings** properties tab. The **Scalable Storage** properties appear only if a cloud storage server is configured. The **Scalable Storage** properties apply to currently selected media servers.

See "Cloud Settings tab of the Scalable Storage properties" on page 22.

Cloud Settings tab of the Scalable Storage properties

The **Cloud Settings** properties contain information about encryption, metering, bandwidth throttling, and network connections between the NetBackup hosts and your cloud storage provider.

The **Cloud Settings** tab appears if the cloud storage service is active on the selected media server.

Figure 2-1 Scalable Storage Cloud Settings host properties

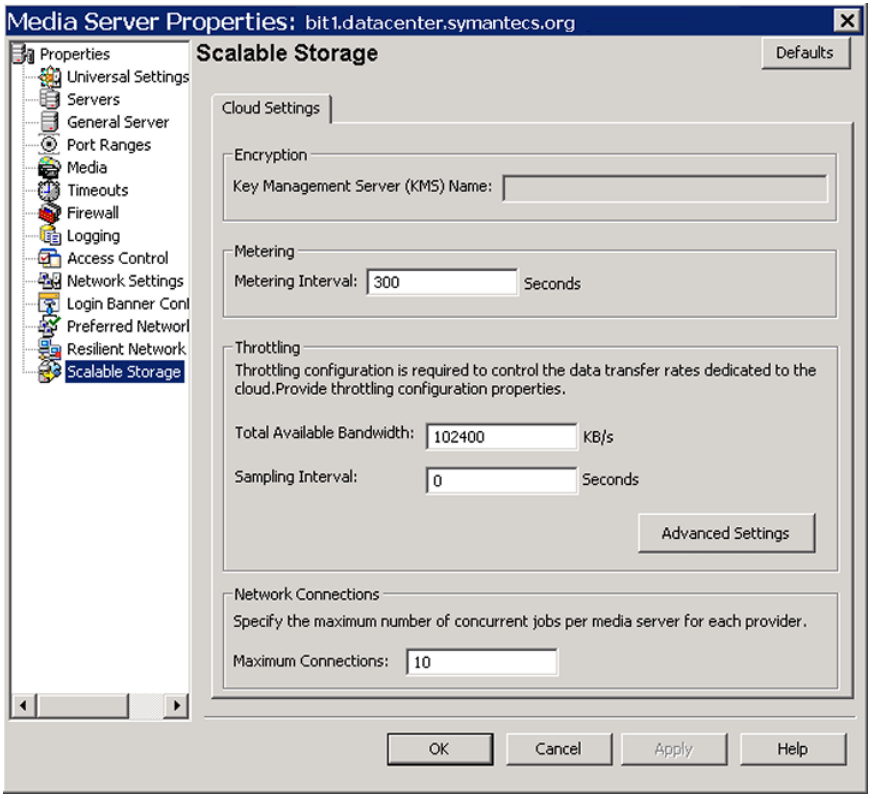


Table 2-6 describes the properties.

Table 2-6 Cloud storage host properties

Property	Description
Key Management Server (KMS) Name	If you configured the NetBackup Key Management Service (KMS), the name of the KMS server.
Metering Interval	Determines how often NetBackup gathers connection information for reporting purposes. NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled.
Total Available Bandwidth	Use this value to specify the speed of your connection to the cloud. The value is specified in kilobytes per second. The default value is 102400 KB/sec.

Table 2-6 Cloud storage host properties *(continued)*

Property	Description
Sampling interval	The time, in seconds, between measurements of bandwidth usage. The larger this value, the less often NetBackup checks to determine the bandwidth in use.
Advanced Settings	Click **Advanced Settings** to specify additional settings for throttling. See "Configuring advanced bandwidth throttling settings" on page 24. See "Advanced bandwidth throttling settings" on page 25.
Maximum connections	The default maximum number of concurrent connections that the media server can open to the cloud storage server. If the maximum number of connections is configured for your cloud storage provider, NetBackup uses that value instead of this default. This value applies to the media server not to the cloud storage server. If you have more than one media server that can connect to the cloud storage server, each media server can have a different value. Therefore, to determine the total number of connections to the cloud storage server, add the values from each media server. If NetBackup is configured to allow more jobs than the number of connections, NetBackup fails any jobs that start after the number of maximum connections is reached. NetBackup retries the failed jobs. If a connection is available when NetBackup retries a failed job, the job does not fail because of a lack of connections. Jobs include both backup and restore jobs. You can configure job limits per backup policy and per storage unit. **Note:** NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of connections per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum. In practice, you should not need to set this value higher than 100.

Configuring advanced bandwidth throttling settings

Advanced bandwidth throttling settings let you control various aspects of the connection between the NetBackup hosts and your cloud storage provider.

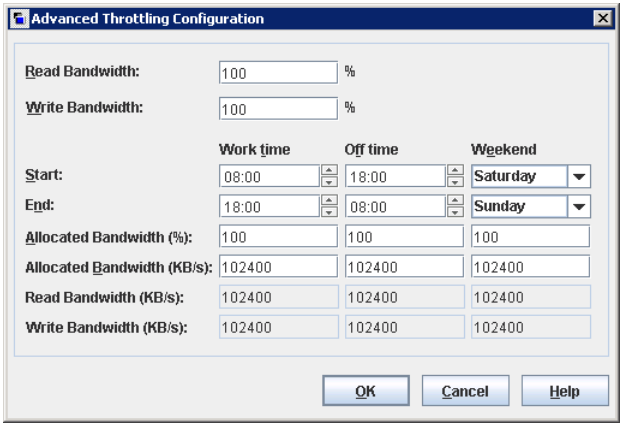
The total bandwidth and the bandwidth sampling interval are configured on the **Cloud Settings** tab of the **Scalable Storage** host properties screen.

See "Scalable Storage properties" on page 22.

To configure advanced bandwidth throttling settings

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Media Servers** in the left pane.
2. In the right pane, select the host on which to specify properties.
3. Click **Actions** > **Properties**.
4. In the properties dialog box left pane, select **Scalable Storage**.
5. In the right pane, click **Advanced Settings**. The **Advanced Throttling Configuration** dialog box appears.

   The following is an example of the dialog box:



6. Configure the settings and then click **OK**.

   See "Advanced bandwidth throttling settings" on page 25.

Advanced bandwidth throttling settings

The following table describes the advanced bandwidth throttling settings.

Table 2-7 Advanced Throttling Configuration settings

Property	Description
Read Bandwidth	Use this field to specify the percentage of total bandwidth that read operations can use. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, restore or replication failures may occur due to timeouts. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth. Default value: `100` Possible values: `0` to `100`
Write Bandwidth	Use this field to specify the percentage of total bandwidth that write operations can use. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth. Default value: `100` Possible values: `0` to `100`
Work time	Use this field to specify the time interval that is considered work time for the cloud connection. Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00. Indicate how much bandwidth the cloud connection can use in the **Allocated bandwidth** field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.

Table 2-7 Advanced Throttling Configuration settings *(continued)*

Property	Description
Off time	Use this field to specify the time interval that is considered off time for the cloud connection. Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00. Indicate how much bandwidth the cloud connection can use in the **Allocated bandwidth** field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.
Weekend	Specify the start and stop time for the weekend. Indicate how much bandwidth the cloud connection can use in the **Allocated bandwidth** field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.
Read Bandwidth (KB/s)	This field displays how much of the available bandwidth the cloud storage server transmits to a NetBackup media server during each restore job. The value is expressed in kilobytes per second.
Write Bandwidth (KB/s)	This field displays how much of the available bandwidth the NetBackup media server transmits to the cloud storage server during backup jobs. The value is expressed in kilobytes per second.

About the NetBackup CloudStore Service Container

The CloudStore Service Container is a Web-based service container that runs on the media server that is configured for cloud storage. This container hosts different services such as the configuration service, the throttling service, and the metering data collector service.

You can configure the CloudStore Service Container behavior by using the **Scalable Storage** host properties in the **NetBackup Administration Console**.

See "Scalable Storage properties" on page 22.

The NetBackup CloudStore Service Container can be started in either secure or non-secure mode. The security mode determines how the clients communicate with the service. Use the `CSSC_IS_SECURE` attribute to set the security mode. The default value is 1, secure communication.

In secure mode, the client components must authenticate with the CloudStore Service Container. After authentication, communication occurs over a secure HTTPS channel. The server generates a self-signed certificate which lasts for 365 days and uses that certificate for authentication. The certificate is named `cssc.crt`. The file is located in the `/usr/openv/lib/ost-plugins` directory on UNIX/Linux and *`install_path`*`\Veritas\NetBackup\bin\ost-plugins` on Windows. If the certificate becomes corrupt or expires, delete the old certificate and restart the services to regenerate a new certificate.

If you change the `CSSC_IS_SECURE` value to zero, the CloudStore Service Container uses non-secure communication. The client communicates with the server over HTTP with no authentication required.

The default port number for the `nbcssc` service is 5637.

See "Stopping and starting the NetBackup CloudStore Service Container" on page 93.

About data encryption for cloud storage

You can encrypt your data before you send it to the cloud.

NetBackup uses the Key Management Service to manage encryption keys. You must configure KMS on the master server so that NetBackup can encrypt data.

See "About key management for encryption of NetBackup cloud storage" on page 28.

More information about data-at-rest encryption and security is available.

See the NetBackup Security and Encryption Guide available from the Symantec Knowledgebase.

About key management for encryption of NetBackup cloud storage

See "About data encryption for cloud storage" on page 28.

NetBackup uses the Key Management Service (KMS) to manage the keys for the data encryption for disk storage. KMS is a NetBackup master server-based symmetric key management service. The service runs on the NetBackup master server. An additional license is not required to use the KMS functionality.

The following table describes the encryption keys that are required for the KMS database.

Table 2-8 Encryption keys required for the KMS database

Key	Description
Host Master Key	The Host Master Key protects the key database. The Host Master Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.
Key Protection Key	A Key Protection Key protects individual records in the key database. The Key Protection Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.

The following table describes the encryption keys that are required for each storage server and volume combination.

Table 2-9 Encryption keys required for each storage server and volume combination

Key	Description
A key group	A key group key protects the key group. Each storage server and volume combination requires a key group. The key group key requires a pass phrase. The key group name must use the following format: *storage_server_name*:*volume_name* The following is the criteria for the key group name: ■ For the *storage_server_name*, you must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server. ■ The colon (:) is required after the *storage_server_name*. ■ For the *volume_name* for cloud storage, you must specify the LSU name that the storage vendor exposes to NetBackup.
A key record	Each key group that you create requires a key record. A key record stores the actual key that protects the data for the storage server and volume.

See "Configuring key management for NetBackup cloud storage encryption" on page 30.

More information about KMS is available.

See the NetBackup Security and Encryption Guide.

See "KMS database encryption settings" on page 45.

Configuring key management for NetBackup cloud storage encryption

For cloud storage, encryption is optional. If you do not use encryption, you do not have to configure key management. To use encryption, Symantec recommends that you use the **Cloud Storage Server Configuration Wizard** and the **Disk Pool Configuration Wizard**. The wizards include the steps that configure key management and encryption.

See "Configuring a storage server for cloud storage" on page 37.

See "Configuring a disk pool for cloud storage" on page 56.

However, you can use NetBackup commands to configure key management manually. This topic describes the process to do so and includes links to the individual tasks you must accomplish.

Table 2-10 Configure key management manually

Step	Task	Instructions
Step 1	Learn about NetBackup key management	See "About key management for encryption of NetBackup cloud storage" on page 28.
Step 2	Set up the KMS database	See "Setting up the KMS database for NetBackup cloud storage encryption" on page 31.
Step 3	Create the key groups	Each storage server and volume combination requires a key group. See "Creating a KMS key group for NetBackup cloud storage" on page 32.
Step 4	Create the key records	Each key group requires a key record. The key record contains the encryption key. See "Creating a KMS key for NetBackup cloud storage encryption" on page 33.
Step 5	Save a record of the key names	The record of the key names lets you recreate the keys if they are lost. See "Saving a record of the KMS key names for NetBackup cloud storage encryption" on page 34.

See "Displaying KMS key information for cloud storage encryption" on page 83.

See "About key management for encryption of NetBackup cloud storage" on page 28.

Setting up the KMS database for NetBackup cloud storage encryption

Setting up the KMS database is the first task in the process of configuring the NetBackup Key Management Service manually.

See "Configuring key management for NetBackup cloud storage encryption" on page 30.

See "KMS database encryption settings" on page 45.

To set up the KMS database

1. On the NetBackup master server, create the KMS database by running the `nbkms` command with the `-createemptydb` option, as follows:

   UNIX: `/usr/openv/netbackup/bin/nbkms -createemptydb`

   Windows: *`install_path`*`\Veritas\NetBackup\bin\nbkms.exe -createemptydb`

   The following prompt appears:

   ```
   Enter the Host Master Key (HMK) passphrase (or hit ENTER to use a
   randomly generated HMK). The passphrase will not be displayed on
   the screen.
   Enter passphrase :
   ```

2. Enter a pass phrase for the host master key (HMK) or press **Enter** to create a randomly generated key.

   After you enter the Host Master Key pass phrase, the following prompt appears:

   ```
   An ID will be associated with the Host Master Key (HMK) just
   created. The ID will assist you in determining the HMK associated
   with any key store.
   Enter HMK ID :
   ```

3. Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.

   After you enter the Host Master Key ID, the following prompt appears:

   ```
   Enter the Key Protection Key (KPK) passphrase (or hit ENTER to
   use a randomly generated KPK). The passphrase will not be
   displayed on the screen.
   Enter passphrase :
   ```

4 Enter a pass phrase for the Key Protection Key or press **Enter** to create a randomly generated key.

After you enter the Key Protection Key pass phrase, the following prompt appears:

```
An ID will be associated with the Key Protection Key (KPK) just
created. The ID will assist you in determining the KPK associated
with any key store.
Enter KPK ID :
```

5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

6 Start the NetBackup Key Management Service on the master server. You can do so in the **Activity Monitor** of the **NetBackup Administration Console**.

After you start the service, the initial database setup is complete.

7 After you set up the database, create key groups for the volumes in the disk pool.

Creating a KMS key group for NetBackup cloud storage

Creating a KMS key group is the second task in the process of configuring the NetBackup Key Management Service manually.

See "Configuring key management for NetBackup cloud storage encryption" on page 30.

See "KMS database encryption settings" on page 45.

A key group is a container for key records. Each storage server and volume combination requires a key group in the following format:

storage_server_name:*volume_name*

To create a KMS key group

1 On the NetBackup master server, create a key group by using the `nbkmsutil` command and the `-createkg` option, as follows:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkg -kgname` *storage_server_name*:*volume_name*

Windows: *install_path*`\Veritas\NetBackup\bin\admincmd\nbkmsutil -createkg -kgname` *storage_server_name*:*volume_name*

The following is the criteria for the key group name:

- For the *storage_server_name*, you must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server.
- The colon (:) is required after the *storage_server_name*.
- For cloud storage, for the *volume_name* you must specify the LSU name that the storage vendor exposes to NetBackup.
  The following example shows the usage for a cloud storage vendor:

  ```
  nbkmsutil -createkg -kgname CloudVendor.com:symc_backups_gold
  ```

2 After you create the key groups, create a key record for each group.

  See "Creating a KMS key for NetBackup cloud storage encryption" on page 33.

Creating a KMS key for NetBackup cloud storage encryption

Creating a KMS key is the third and the final task in the process of configuring the NetBackup Key Management Service manually.

See "Configuring key management for NetBackup cloud storage encryption" on page 30.

See "KMS database encryption settings" on page 45.

Each key group requires at least one *key record*. The key record contains the encryption key itself and information about the key. The key is used to encrypt and decrypt data.

Note: If you create more than one key for a key group, only the last key remains active.

To create a KMS key

1 On the NetBackup master server, create a key record by using the `nbkmsutil` command and the `-createkey` option.

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkey -keyname keyname -kgname key_group_name -activate`

Windows: `install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil -createkey -keyname keyname -kgname key_group_name -activate`

The following example shows the usage for a cloud storage vendor:

```
nbkmsutil -createkey -keyname Encrypt_Key_April -kgname
CloudVendor.com:symc_backups_gold -activate
```

You are prompted to enter a pass phrase:

```
Enter a passphrase:
```

2 Enter and then re-enter a pass phrase; this pass phrase should differ from any pass phrases that you entered already.

3 Save a record of the pass phrase.

See "Saving a record of the KMS key names for NetBackup cloud storage encryption" on page 34.

Saving a record of the KMS key names for NetBackup cloud storage encryption

Symantec recommends that you save a record of the encryption key names. The key tag that is listed in the output is necessary if you need to recover or recreate the keys.

To save a record of the key names

1 To determine the key group names, use the following command on the master server:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs`

Windows: *`install_path`*`\Program Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkgs`

The following is example output:

```
Key Group Name         : CloudVendor.com:symc_backups_gold
Supported Cypher       : AES_256
Number of Keys         : 1
Has Active Key         : Yes
Creation Time          : Tues Oct 01 01:00:00 2013
Last Modification Time: Tues Oct 01 01:00:00 2013
Description            : CloudVendor.com:symc_backups_gold
```

2 For each key group, write all of the keys that belong to the group to a file. Run the command on the master server. The following is the command syntax:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname key_group_name > filename.txt`

Windows: `install_path\Program Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkeys -kgname key_group_name > filename.txt`

The following is example output:

```
nbkmsutil.exe -listkeys -kgname CloudVendor.com:symc_backups_gold
> encrypt_keys_CloudVendor.com_symc_backups_gold.txt
```

```
Key Group Name        : CloudVendor.com:symc_backups_gold
Supported Cypher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : Key group to protect cloud volume

  Key Tag      : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
  Key Name              : Encrypt_Key_April
  Current State         : Active
  Creation Time         : Tues Jan 01 01:02:00 2013
  Last Modification Time: Tues Jan 01 01:02:00 2013
  Description           : -

Number of Keys: 1
```

3 Include in the file the passphrase that you used to create the key record.

4 Store the file in a secure location.

About cloud storage servers

A storage server is an entity that writes data to and reads data from the storage. For cloud storage, it is usually a host on the Internet to which you send the backup data. Your storage vendor provides the name of the storage server. Use that name when you configure cloud storage in NetBackup.

Only one storage servers exists in a NetBackup domain for a specific storage vendor.

If you share the backup images on a cloud vendor's storage, you must configure a storage server in each NetBackup domain that shares the backup images.

Other NetBackup media servers back up the clients and move the data to the storage server.

See "About cloud storage data movers" on page 67.

Configuring a storage server for cloud storage

Configure in this context means to configure a host as a storage server that can write to and read from the cloud storage. The NetBackup **Cloud Storage Server Configuration Wizard** communicates with your cloud storage vendor's network and selects the appropriate host for the storage server. The wizard also lets you configure the NetBackup Key Management Service for encryption.

At least one media server must be enabled for cloud storage. To be enabled for cloud storage, a NetBackup media server must meet the following conditions:

- The media server operating system must be supported for cloud storage.
  For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list on the Symantec NetBackup Support Landing Page.
- The NetBackup CloudStore Service Container (`nbcssc`) must be running.
- The cloud storage binary files must be present in the `ost-plugins` directory.

NetBackup supports private the clouds from the supported cloud providers.

See "About private clouds from supported cloud vendors" on page 21.

See "About cloud storage servers" on page 36.

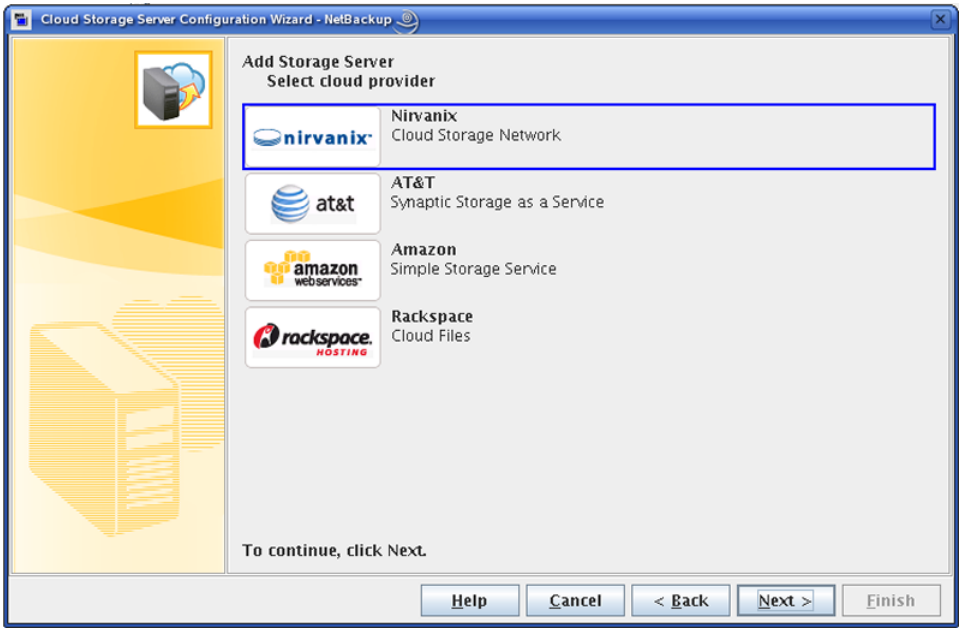
To configure a cloud storage server by using the wizard

1. In the **NetBackup Administration Console** connected to the NetBackup master server, select either **NetBackup Management** or **Media and Device Management**.
2. In the right pane, click **Configure Cloud Storage Servers**.

3 Click **Next** on the welcome panel of the wizard.

The **Select Cloud Provider** panel appears.

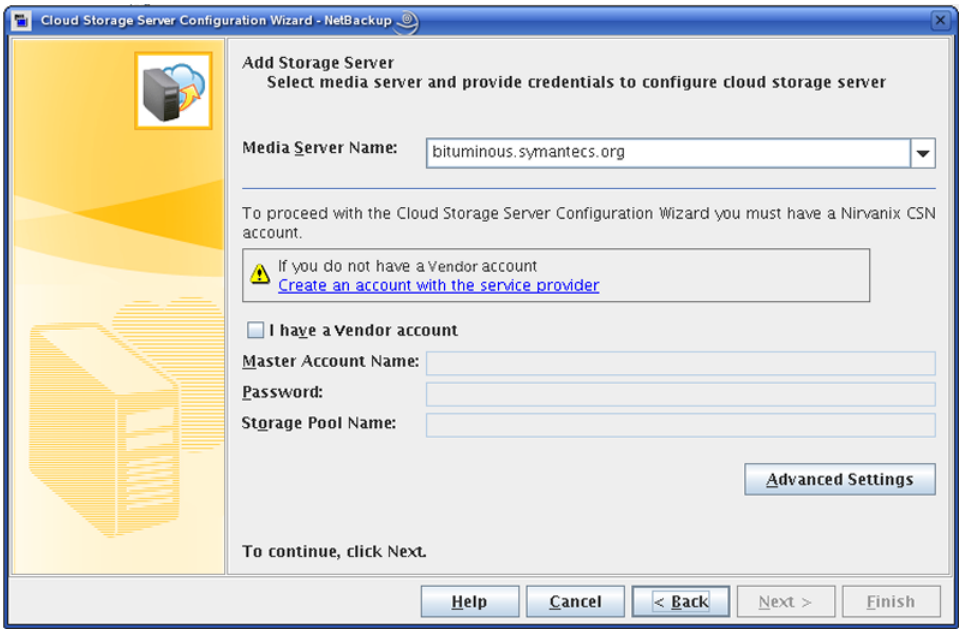
The following is an example of the wizard panel:



4 On the **Select Cloud Provider** panel, select your cloud storage provider and then click **Next**.

After you click **Next**, a cloud storage provider configuration panel appears.

The following is an example of a configuration panel.



5 On the **Select media server** panel, do the following:

a Select the media server to use to query the storage server. It must be a media server that is enabled for cloud storage.

b If you do not have a storage provider account, click **Create an account with service provider** on the storage provider configuration panel. Use the web browser that opens to create an account with the storage provider. Save the information so that you can use it to complete this wizard panel.

If you configure a private cloud, the webpage that opens has no value for your configuration process.

c For the **I have a *VendorName* account** option, do one of the following:

- For public cloud storage, click **I have a *VendorName* account**.
- To configure a private cloud using the cloud storage vendor's protocols, clear the **I have a *VendorName* account** check box.
  See "About private clouds from supported cloud vendors" on page 21.

d To configure the cloud storage server with the default options for the cloud storage vendor, select or enter the options in this wizard panel. The options that you have to configure depend on the storage provider. They also depend on if you configure a private cloud.

See "Amazon S3 storage server configuration options" on page 43.

See "AT&T storage server configuration options" on page 43.

See "Rackspace storage server configuration options" on page 44.

e To configure the cloud storage server with options other than the default or to configure a private cloud, click **Advanced**. Then, do the following on the **Advanced Server Configuration** dialog box:

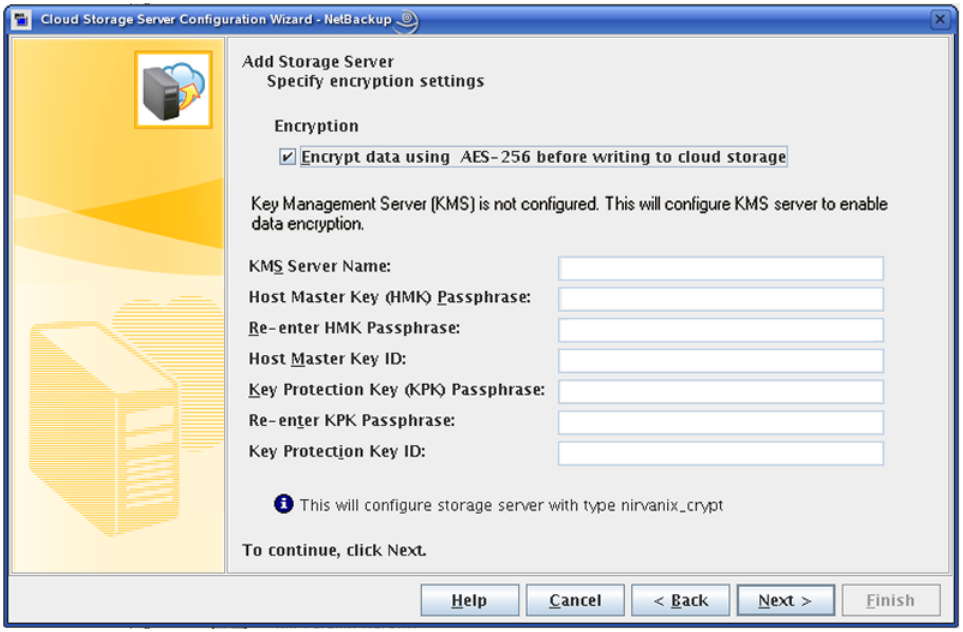
- To change the storage server, click **Override storage server** and then enter the storage server name.
  You can use this option to specify an internal host for a private cloud.
- To limit the number of simultaneous network connections to the storage server, enter the value in the **Maximum Connections** box. If you do not set the value here, NetBackup uses the global value from the Cloud Storage host properties.
  See "Scalable Storage properties" on page 22.

f Click **OK** in the **Advanced Server Configuration** dialog box.

g Click **Next** in the **Select media server** panel.

The **Specify Encryption Settings** panel appears.

The following is an example of the panel:

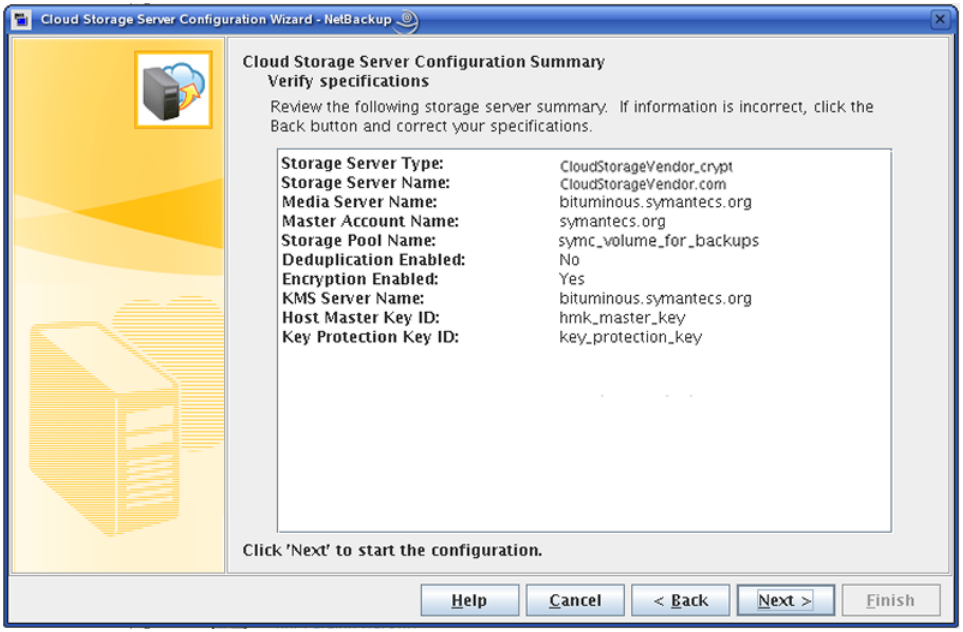

Cloud Storage Server Configuration Wizard - NetBackup
Add Storage Server
Specify encryption settings
Encryption
Encrypt data using AES-256 before writing to cloud storage
Key Management Server (KMS) is not configured. This will configure KMS server to enable data encryption.
KMS Server Name:
Host Master Key (HMK) Passphrase:
Re-enter HMK Passphrase:
Host Master Key ID:
Key Protection Key (KPK) Passphrase:
Re-enter KPK Passphrase:
Key Protection Key ID:
This will configure storage server with type nirvanix_crypt
To continue, click Next.
Help
Cancel
< Back
Next >
Finish

6 On the **Specify Encryption Settings** panel, select or enter the encryption settings.

See “KMS database encryption settings” on page 45.

After you click **Next**, the **Cloud Storage Server Configuration Summary** panel appears.

The following is an example of the panel:



7 On the **Cloud Storage Server Configuration Summary** panel, verify the selections. If OK, click **Next**. If not OK, click **Back** until you reach the panel on which you need to make corrections.

8 After the wizard creates the storage server, click **Next**.

The **Storage Server Creation Confirmation** panel appears.

9 On the **Completion** panel, do one of the following:

To continue to the **Disk Pool Configuration Wizard**, click **Next**.

See “Configuring a disk pool for cloud storage” on page 56.

To exit from the wizard, click **Close**.

Amazon S3 storage server configuration options

The following table describes the storage server configuration options for Amazon S3.

Table 2-11 Amazon S3 storage server configuration options

Field name	Required content
Media Server Name	Select NetBackup media server from the drop-down list. Only those media servers that are enabled for cloud storage appear in the list, as follows: ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (`nbcssc`) must be running. ■ The cloud storage binary files must be present in the `ost-plugins` directory. The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores. See "About cloud storage data movers" on page 67. After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.
I have an Amazon S3 account	Select **I have a Amazon S3 account** (Cloud Storage Network) to enter the required account information.
Access ID	Enter your Amazon S3 Access ID. If you do not have an account, click **Create an account with the service provider** link.
Secure Access Token	Enter your Amazon S3 Secure Access Token.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

AT&T storage server configuration options

The following table describes the storage server configuration options for AT&T.

Table 2-12 AT&T Storage server configuration options

Field name	Required content
Media Server Name	Select NetBackup media server from the drop-down list. Only those media servers that are enabled for cloud storage appear in the list, as follows: ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (`nbcssc`) must be running. ■ The cloud storage binary files must be present in the `ost-plugins` directory. The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores. See "About cloud storage data movers" on page 67. After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.
I have an AT&T Synaptic storage account	Select **I have an AT&T Synaptic storage account** to enter the required account information.
User Name	Enter your AT&T user name. If you do not have an account, click **Create an account with the service provider** link.
Password	Enter the password for the **User Name** account.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

Rackspace storage server configuration options

The following table describes the storage server configuration options for Rackspace.

Table 2-13 Rackspace storage server configuration options

Field name	Required content
Media Server Name	Select a NetBackup media server from the drop-down list. Only those media servers that are enabled for cloud storage appear in the list, as follows: ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (`nbcssc`) must be running. ■ The cloud storage binary files must be present in the `ost-plugins` directory. The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores. See "About cloud storage data movers" on page 67. After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plug-in design. Attempts to change the media server generate an authorization error.
I have a Rackspace Cloud Files account	Select **I have a Rackspace Cloud Files account** to enter the required account information.
User Name	Enter your Rackspace Cloud Files account user name. If you do not have an account, click **Create an account with the service provider** link.
Access Key	Enter your Rackspace Cloud Files account access key.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

KMS database encryption settings

The following table describes the settings to configure the NetBackup Key Management Service database.

Table 2-14 Required information for the encryption database

Field Name	Required information
KMS Server Name	This field displays the name of your NetBackup master server. You can only configure KMS on your master server. This field cannot be changed. If KMS is not configured, this field displays **<kms_server_name>**.
Host Master Key (HMK) Passphrase	Enter the key that protects the database. In KMS terminology, the key is called a *passphrase*.

Table 2-14 Required information for the encryption database *(continued)*

Field Name	Required information
Re-enter HMK Passphrase	Re-enter the host master key.
Host Master Key ID	The ID is a label that you assign to the master key. The ID lets you identify the particular host master key. You are limited to 255 characters in this field. To decipher the contents of a keystore file, you must identify the correct Key Protection Key and Host Master Key. These IDs are stored unencrypted in the keystore file header. You can select the correct ones even if you only have access to the keystore file. To perform a disaster recovery you must remember the correct IDs and passphrases that are associated with the files.
Key Protection Key (KPK) Passphrase	Enter the password that protects the individual records within the KMS database. In KMS terminology, the key is called a *passphrase*.
Re-enter KPK Passphrase	Re-enter the key protection password.
Key Protection Key ID	The ID is a label that you assign to the key. The ID lets you identify the particular key protection key. You are limited to 255 characters in this field. To decipher the contents of a keystore file, you must identify the correct Key Protection Key and Host Master Key. These IDs are stored unencrypted in the keystore file header. You can select the correct ones even if you only have access to the keystore file. To perform a disaster recovery you must remember the correct IDs and passphrases that are associated with the files.

Key groups and key records also are required for encryption. If you use the NetBackup wizards to configure cloud storage, the **Disk Pool Configuration Wizard** configures them for you. If you use the

See "Configuring key management for NetBackup cloud storage encryption" on page 30.

See "About key management for encryption of NetBackup cloud storage" on page 28.

Cloud storage server properties

The **Properties** tab of the **Change Storage Server** dialog box lets you change some of the properties that affect the NetBackup interaction with the cloud storage.

Not all properties apply to all storage vendors.

Table 2-15 describes the prefixes for the various properties.

Table 2-15 Prefix definitions

Prefix	Prefix meaning
AMZ	Amazon
ATT	AT&T
COMPR	Data compression
CRYPT	Encryption
METER	Metering
RACKS	Rackspace
THR	Throttling

See "Storage server cloud connection properties" on page 47.

See "Storage server bandwidth throttling properties" on page 50.

See "Storage server encryption properties" on page 54.

Storage server cloud connection properties

All or most of the storage vendors use the storage server properties in Table 2-16. The following are the prefixes for the currently supported cloud vendors:

- Amazon: AMZ
- AT&T: ATT
- Rackspace: RACKS

Table 2-16 Storage server cloud connection properties

Property	Description
METER:DIRECTORY	This read-only field displays the directory in which to store data stream metering information. Default value: /usr/openv/lib/ost-plugins/meter (UNIX) or *install_path*\VERITAS\NetBackup\bin\ost-plugins\ (Windows)

Table 2-16 Storage server cloud connection properties *(continued)*

Property	Description
METER:INTERVAL	The interval at which NetBackup gathers connection information for reporting purposes. NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled To change this property, use the **Cloud Settings** tab of the **Scalable Storage** host properties. See "Cloud Settings tab of the Scalable Storage properties" on page 22. Default value: 300 Possible values: 1 to 10000
PREFIX:CURL_CONNECT_TIMEOUT	The amount of time that is allocated for the media server to connect to the cloud storage server. This value is specified in seconds. The default is 300 seconds or five minutes. The media server makes three attempts to connect out during the specified time. This only limits the connection time, not the session time. If the media server cannot connect to the cloud storage server in the specified time, the job fails. This value cannot be disabled. If an invalid number is entered, the CURL_CONNECT_TIMEOUT returns to the default value of 300. In addition to the CURL_CONNECT_TIMEOUT that is a global value, you can set a cURL timeout value for each cloud vendor. If these values are set, they apply only to the specified vendor. If both the global value and the vendor-specific values are set, the vendor-specific value takes precedent. Default value: 300 Possible values: 1 to 10000
PREFIX:CURL_TIMEOUT	The maximum time in seconds to allow for the completion of a data operation. This value is specified in seconds. If the operation does not complete in the specified time, the operation fails. The default is 900 seconds (15 minutes). The media server attempts the operation up to three times. To disable this timeout, set the value to 0 (zero). Default value: 900 Possible values: 1 to 10000

Table 2-16 Storage server cloud connection properties *(continued)*

Property	Description
PREFIX:LOG_CURL	Determines if cURL activity is logged. The default is NO which means log activity is disabled. Default value: NO Possible values: NO (disabled) and YES (enabled)
PREFIX:PROXY_IP	The TCP/IP address of the proxy server. If you do not use a proxy server, leave this field blank. Default value: No default Possible values: Valid TCP/IP address
PREFIX:PROXY_PORT	The port number that is used to connect to the proxy server. The default is 70000 which indicates you do not use a proxy server. Default value: 70000 Possible values: Valid port number
PREFIX:PROXY_TYPE	Used to define the proxy server type. If a firewall prevents access to your cloud vendor, use this value to define your proxy server type. If you do not use a proxy server, leave this field blank. Default value: NONE Possible values: NONE, HTTP, SOCKS, SOCKS4, SOCKS5, SOCKS4A
PREFIX:READ_BUFFER_SIZE	The size of the buffer to use for read operations. The default is 0 and the value is specified in bytes. To enable the use of the buffer, set this value to a non-zero number. Symantec recommends that this value be a multiple of 256. The READ_BUFFER_SIZE determines the size of the data packets that the storage server transmits during each restore job. An increase in the value may increase performance when a large amount of contiguous data is accessed. If insufficient bandwidth exists to transmit the specified amount of data within a few minutes, restore failures may occur due to timeouts. When you calculate the required bandwidth, consider the total load of simultaneous backup jobs and restore jobs on multiple media servers. Default value: 0 Possible values: 524288 (512 KB) to 1073741824 (1 GB)

Table 2-16 Storage server cloud connection properties *(continued)*

Property	Description
PREFIX:USE_SSL	Determines if Secure Sockets Layer encryption is used for the control APIs. The default value is YES, meaning SSL is enabled. Default value: YES Possible values: YES or NO
PREFIX:USE_SSL_RW	Determines if Secure Sockets Layer encryption is used for read and write operations. The default value is YES, meaning SSL is enabled. Default value: YES Possible values: YES or NO
PREFIX:WRITE_BUFFER_NUM	This read-only field displays the total number of write buffers that are used by the plug-in. The WRITE_BUFFER_SIZE value defines the size of the buffer. The value is set to 1 and cannot be changed. Default value: 1 Possible values: 1
PREFIX:WRITE_BUFFER_SIZE	The size of the buffer to use for write operations. The value is specified in bytes. The default is 10485760 (10 MBs). Valid values are 0 to 1073741824 (1 GB). To disable the use of the buffer, set this value to 0 (zero). The WRITE_BUFFER_SIZE value determines the size of the data packs transmitted from the data mover to the storage server during a backup. An increase in the value may increase performance when a large amount of contiguous data is accessed. If insufficient bandwidth exists to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts. When you calculate the required bandwidth, consider the total load of simultaneous backup jobs and restore jobs on multiple media servers. Default value: 10485760 Possible values: 10485760 (10 MB) to 1073741824 (1 GB)

See "Changing storage server properties in NetBackup" on page 65.

See "Cloud storage server properties" on page 46.

Storage server bandwidth throttling properties

The following storage server properties apply to bandwidth throttling. The THR prefix specifies a throttling property. Use the correct cloud provider URL for the desired cloud vendor.

To change these properties, use the **Scalable Storage** host properties **Cloud Settings** tab.

See "Cloud Settings tab of the Scalable Storage properties" on page 22.

Table 2-17 Cloud storage server bandwidth throttling properties

Property	Description
THR:*storage_server*	Shows the storage server name for specified cloud storage server. Possible values for *storage_server* are: ■ Amazon: amazon.com ■ AT&T: storage.synaptic.att.com ■ Rackspace: rackspace.com Default value: Not applicable Possible values: See Description
THR:AVAIL_BANDWIDTH	This read-only field displays the total available bandwidth value for the cloud feature. The value is displayed in bytes per second. You must specify a number greater than zero. If you enter zero, an error is generated. Default value: 104857600 Possible values: Any positive integer

Table 2-17 Cloud storage server bandwidth throttling properties *(continued)*

Property	Description
THR:DEFAULT_MAX_CONNECTIONS	The default maximum number of concurrent connections that the media server can open to the cloud storage server. If the maximum number of connections is configured for your cloud storage provider, NetBackup uses that value instead of this default. This read-only field displays the maximum number of concurrent connections that the media server can open to the cloud storage server. This value applies to the media server not to the cloud storage server. If you have more than one media server that can connect to the cloud storage server, each media server can have a different value. Therefore, to determine the total number of connections to the cloud storage server, add the values from each media server. If NetBackup is configured to allow more jobs than the number of connections, NetBackup fails any jobs that start after the number of maximum connections is reached. NetBackup retries the failed jobs. If a connection is available when NetBackup retries a failed job, the job does not fail because of a lack of connections. Jobs include both backup and restore jobs. You can configure job limits per backup policy and per storage unit. **Note:** NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of connections per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum. In practice, you should not need to set this value higher than 100. Default value: 10 Possible values: 1 to 2147483647
THR:OFF_TIME_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during off time. Default value: 100 Possible values: 0 to 100
THR:OFF_TIME_END	This read-only field displays the end of off time. Specify the time in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 8 Possible values: 0 to 2359

Table 2-17 Cloud storage server bandwidth throttling properties *(continued)*

Property	Description
THR:OFF_TIME_START	This read-only field displays the start of off time. Specify the time in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 18 Possible values: 0 to 2359
THR:READ_BANDWIDTH_PERCENT	This read-only field displays the read bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated. Default value: 100 Possible values: 0 to 100
THR:SAMPLE_INTERVAL	This read-only field displays the rate at which backup streams sample their utilization and adjust their bandwidth use. The value is specified in seconds. When this value is set to zero, throttling is disabled. Default value: 0 Possible values: 1 to 2147483647
THR:WEEKEND_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during the weekend. Default value: 100 Possible values: 0 to 100
THR:WEEKEND_END	This read-only field displays the end of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on. Default value: 7 Possible values: 1 to 7
THR:WEEKEND_START	This read-only field displays the start of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on. Default value: 6 Possible values: 1 to 7
THR:WORK_TIME_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during the work time. Default value: 100 Possible values: 0 to 100

Table 2-17 Cloud storage server bandwidth throttling properties *(continued)*

Property	Description
THR:WORK_TIME_END	This read-only field displays the end of work time. Specify the time in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 18 Possible values: 0 to 2359
THR:WORK_TIME_START	This read-only field displays the start of work time. Specify the time in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 8 Possible values: 0 to 2359
THR:WRITE_BANDWIDTH_PERCENT	This read-only field displays the write bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated. Default value: 100 Possible values: 0 to 100

See "Changing storage server properties in NetBackup" on page 65.

See "Cloud storage server properties" on page 46.

Storage server encryption properties

The following encryption-specific storage server properties are used by all or most of the storage vendors. The CRYPT prefix specifies an encryption property. These values are for display purposes only and cannot be changed.

Table 2-18 Encryption cloud storage server properties

Property	Description
CRYPT:KMS_SERVER	This read-only field displays NetBackup server that hosts the KMS service. When you set the storage server properties, enter the name of the KMS server host. By default, this field contains the NetBackup master server name. You cannot change this value. Default value: The NetBackup master server name Possible values: N/A

Table 2-18 Encryption cloud storage server properties *(continued)*

Property	Description
CRYPT:KMS_VERSION	This read-only field displays the NetBackup Key Management Service version. You cannot change this value. Default value: 16 Possible values: N/A
CRYPT:LOG_VERBOSE	This read-only field displays if logs are enabled for encryption activities. The value is either YES for logging or NO for no logging. Default value: NO Possible values: YES and NO
CRYPT:VERSION	This read-only field displays the encryption version. You cannot change this value. Default value: 13107 Possible values: N/A

See "Changing storage server properties in NetBackup" on page 65.

See "Cloud storage server properties" on page 46.

About cloud storage disk pools

A disk pool represents disk volumes on the underlying disk storage. A disk pool is the storage destination of a NetBackup storage unit. For cloud storage, you must specify only one volume for a disk pool.

Disk pool and disk volume names must be unique within your cloud storage provider's environment.

If you share NetBackup images among multiple NetBackup domains, you do not have to use the same disk pool name in each domain. However, you must use the same volume that you configured in the primary sharing domain.

If a cloud storage disk pool is a storage destination in a storage lifecycle policy, NetBackup capacity management applies.

See "Configuring a disk pool for cloud storage" on page 56.

Configuring a disk pool for cloud storage

Symantec recommends that you use the **Disk Pool Configuration Wizard** to create a disk pool.

See "To configure a cloud storage disk pool by using the wizard" on page 56.

Alternatively, you can use the NetBackup `nbdevconfig` command configure a disk pool.

See "To configure a cloud storage disk pool by using the nbdevconfig command" on page 63.

When you create encrypted storage, you must enter a pass phrase for each selected volume that uses encryption. The pass phrase creates the encryption key for that volume.

To configure a cloud storage disk pool by using the wizard

1. If the **Disk Pool Configuration Wizard** was launched from the **Storage Server Configuration Wizard**, go to step 6.

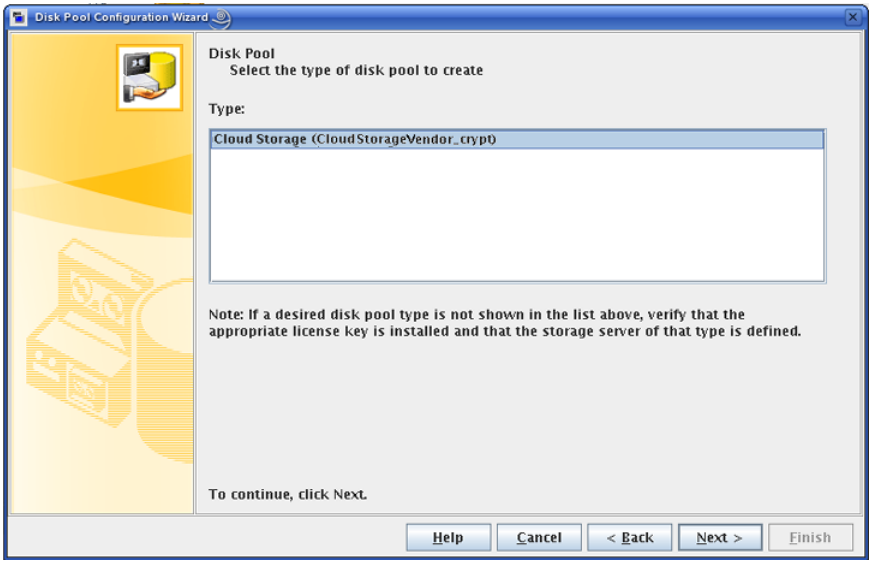
   Otherwise, in the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.

2. From the list of wizards in the right pane, click **Configure Disk Pool**.

3 Click **Next** on the welcome panel of the wizard.

The **Disk Pool** panel appears.

The following is an example of the wizard panel:

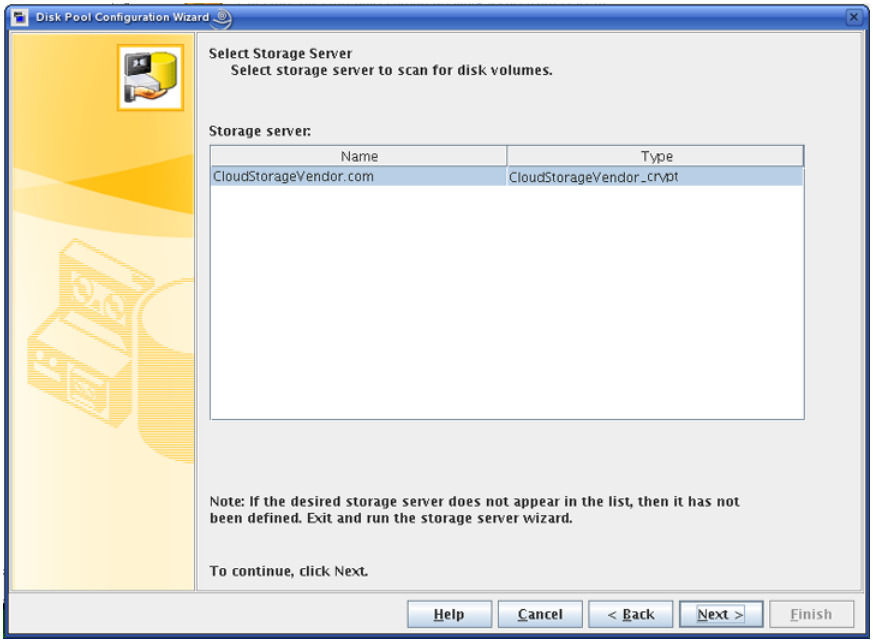


4 On the **Disk Pool** panel, select your storage vendor disk pool type, as follows:

The types of disk pools that you can configure depend on the options for which you are licensed.

Click **Next**. The **Select Storage Server** wizard panel appears.

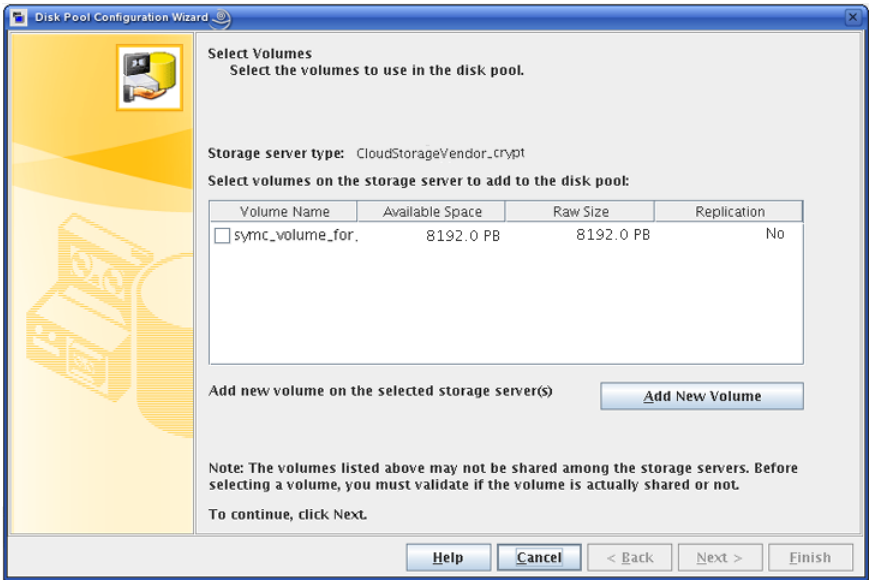
The following is an example of the wizard panel:



5 On the **Select Storage Server** panel, select the storage server for this disk pool. The wizard displays the deduplication storage servers that are configured in your environment.

Click **Next**. A wizard panel on which you select storage volumes appears.

The following is an example of the wizard panel:



6 On the **Create Volumes** panel, select the volume for this disk pool. You must select only one volume for a disk pool.

If no volumes are available, click **Add New Volume**. A **Create Cloud Storage Volume** dialog box appears. The information that is required for the new volume depends on your storage provider.

After you create the new volume, select the volume and then click **Next**.

If you select a volume on a storage destination that does not require encryption, the **Disk Pool Properties** panel appears. Go to step 8.

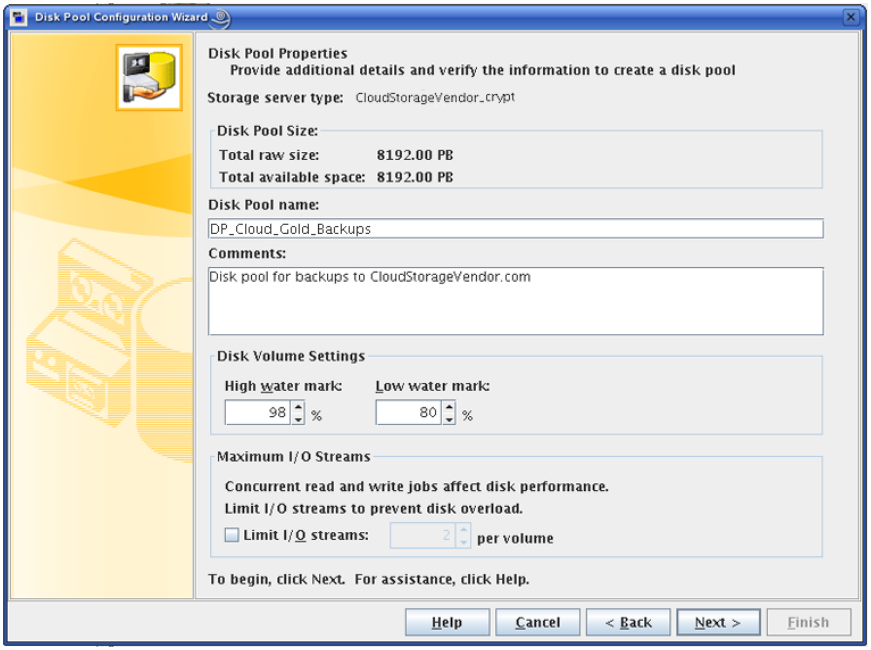
If you select a volume on a storage destination that requires encryption, a dialog box appears in which you must enter the encryption pass phrase. The pass phrase is for the key group for this storage. Continue to the next step.

7 For encrypted storage, enter the pass phrase for the key group in the **Settings** dialog box, then click **OK**.

See "About key management for encryption of NetBackup cloud storage" on page 28.

Click **Next**. The **Disk Pool Properties** wizard panel appears.

The following is an example of the wizard panel:

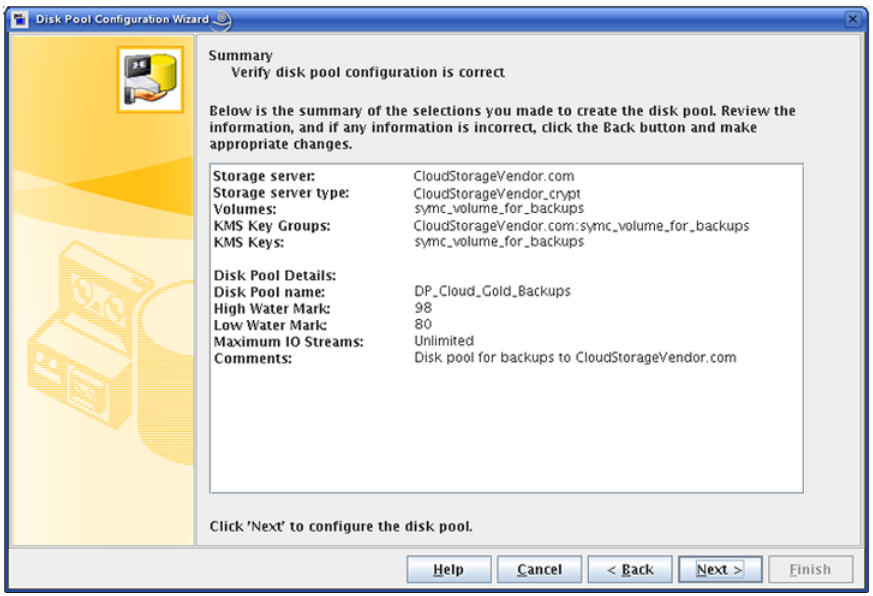


8 On the **Disk Pool Properties** panel, enter the values for this disk pool.

See “Cloud storage disk pool properties” on page 79.

Click **Next**. The **Summary** panel appears.

The following is an example of the wizard panel:



9 On the **Summary** panel, verify the selections. Also, save the KMS key group name and the KMS key name. They are required to recover the keys.

See “Saving a record of the KMS key names for NetBackup cloud storage encryption” on page 34.

If the summary shows your selections accurately, click **Next**.

10 After NetBackup creates the disk pool, a wizard panel describes the successful action.

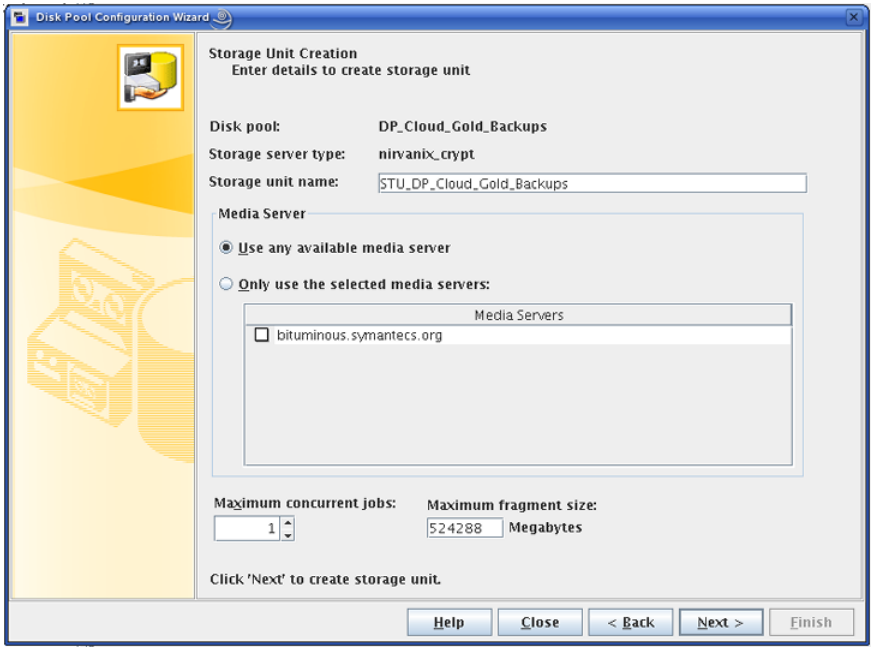
To continue, click **Next**.

The **Storage Unit Creation** wizard panel appears.

11 To configure a storage unit for the disk pool, ensure that **Create a storage unit that uses *disk_pool_name*** is selected, then click **Next**. Otherwise, click **Close** to exit from the wizard.

If you click **Next**, a wizard panel appears in which you enter the details about the storage unit.

The following is an example of the wizard panel:



12 Enter the appropriate information for the storage unit.

See “Cloud storage unit properties” on page 69.

Click **Next** to create the storage unit.

You can use storage unit properties to control your backup traffic.

See “Configure a favorable client-to-server ratio” on page 71.

See “Control backup traffic to the media servers” on page 72.

13 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

To configure a cloud storage disk pool by using the nbdevconfig command

1. On the NetBackup master server, discover the volumes that are available and write them to a text file. The following is the NetBackup command to use, depending on your operating system:

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers hostname -stype server_type > filename`

   Windows: `install_path\NetBackup\bin\admincmd\nbdevconfig -previewdv -storage_servers hostname -stype server_type > filename`

   See "Cloud disk pool options for the nbdevconfig command" on page 64.

2. In a text editor, delete the line for each volume that you do not want to be in the disk pool. Do not delete the blank line at the end of the file.

3. For encrypted storage, configure the key group and key record for this storage. Use the volume name returned by the `nbdevconfig -previewdv` command for the `volume_name` portion of the key group name.

   See "About key management for encryption of NetBackup cloud storage" on page 28.

   See "Creating a KMS key group for NetBackup cloud storage" on page 32.

   See "Creating a KMS key for NetBackup cloud storage encryption" on page 33.

4. Configure the disk pool by using the following command, depending on your operating system:

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp disk_pool_name -stype server_type -storage_servers hostname -dvlist filename [-reason "string"] [-lwm low_watermark_percent] [-max_io_streams n] [-comment comment] [-M master_server] [-reason "string"]`

   Windows: `install_path\NetBackup\bin\admincmd\nbdevconfig -createdp -dp disk_pool_name -stype server_type -storage_servers hostname -dvlist filename [-reason "string"] [-lwm low_watermark_percent] [-max_io_streams n] [-comment comment] [-M master_server] [-reason "string"]`

   See "Cloud disk pool options for the nbdevconfig command" on page 64.

5. After you configure the disk pool, configure a storage unit.

   See "Configuring a storage unit for cloud storage" on page 68.

Cloud disk pool options for the nbdevconfig command

The following describe the options:

Table 2-19 Cloud disk pool options for the nbdevconfig command

-comment *comment*	A comment that is associated with the disk pool.
-dp *disk_pool_name*	The name of the disk pool. Use the same name that you used when you configured the disk volumes.
-dvlist *filename*	The name of the file that contains the information about the volumes for the disk pool.
filename	The name of the file into which to write the volume information. Symantec recommends that you use a name that describes its purpose.
-hwm *high_watermark*	The *high_watermark* setting is a threshold that triggers the following actions: ■ When an individual volume in the disk pool reaches the *high_watermark*, NetBackup considers the volume full. NetBackupchooses a different volume in the disk pool to write backup images to. ■ When all volumes in the disk pool reach the *high_watermark*, the disk pool is considered full. NetBackup fails any backup jobs that are assigned to a storage unit in which the disk pool is full. NetBackup also does not assign new jobs to a storage unit in which the disk pool is full. ■ NetBackup begins image cleanup when a volume reaches the *high_watermark*; image cleanup expires the images that are no longer valid. For a disk pool that is full, NetBackup again assigns jobs to the storage unit when image cleanup reduces any disk volume's capacity to less than the *high_watermark*. The default is 98%.
-lwm *low_watermark*	The *low_watermark* is a threshold at which NetBackup stops image cleanup. The *low_watermark* setting cannot be greater than or equal to the *high_watermark* setting. The default is 80%.
-M *master_server*	The name of the master server.

Table 2-19 Cloud disk pool options for the nbdevconfig command *(continued)*

`-max_io_streams n`	Select to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit. When the limit is reached, NetBackup chooses another volume for write operations, if available. If not available, NetBackup queues jobs until a volume is available. Too many streams may degrade performance because of disk thrashing. Disk thrashing is excessive swapping of data between RAM and a hard disk drive. Fewer streams can improve throughput, which may increase the number of jobs that complete in a specific time period. A starting point is to divide the **Maximum concurrent jobs** of all of the storage units by the number of volumes in the disk pool.
`-reason "string"`	The reason that you create the disk pool.
`-storage_servers hostname`	For the public storage from a supported vendor, enter one of the following: ■ `amazon.com` ■ `rackspace.com` ■ `storage.synaptic.att.com` For the private storage from a supported vendor, enter the name of your host that provides the cloud functionality.
`-stype server_type`	For the type of storage, enter one of the following depending on the vendor and whether or not the storage is encrypted: ■ `amazon_crypt` ■ `amazon_raw` ■ `att_crypt` ■ `att_raw` ■ `rackspace_crypt` ■ `rackspace_raw`

Changing storage server properties in NetBackup

You can change the properties of your storage server. Normally, you should not have to change the properties.

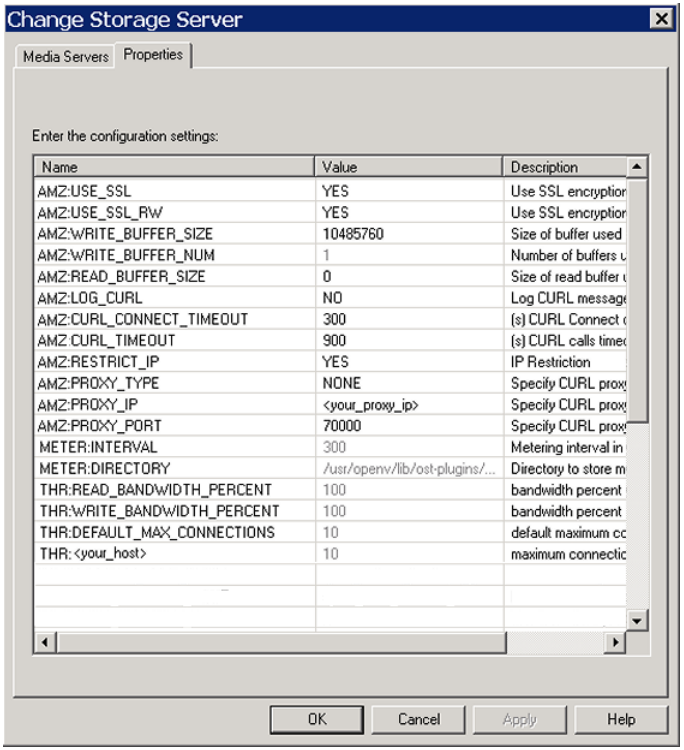
The storage vendor exposes the properties that you can change.

See "Configuring cloud storage in NetBackup" on page 14.

To change storage server properties

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**.
2. Select the storage server.
3. On the **Edit** menu, select **Change**.
4. In the **Change Storage Server** dialog box, select the **Properties** tab.

   The following is an example of the **Properties** for a cloud storage server:



5. To change a property, select its value in the **Value** column and then change it.

   See “Cloud storage server properties” on page 46.

   See “Storage server cloud connection properties” on page 47.

   See “Storage server encryption properties” on page 54.
6. Repeat step 5 until you have finishing changing properties.

7 Click **OK**.

8 Restart the `nbrmms` service by using the **NetBackup Administration Console Activity Monitor**.

About cloud storage data movers

A data mover is a NetBackup media server that backs up a client and then transfers the data to a storage server. The storage server then writes the data to storage. A data mover also can move data back to primary storage (the client) during restores and from secondary storage to tertiary storage during duplication.

When you configure a cloud storage server, the media server that you specify in the wizard or on the command line becomes a data mover. That media server is used to back up your client computers.

You can add additional media servers. They can help balance the load of the backups that you send to the cloud storage. The media servers that you add are assigned the credentials for the storage server. The credentials allow the data movers to communicate with the storage server.

The data movers host a software plug-in that they use to communicate with the storage implementation.

See "Adding backup media servers to your cloud environment" on page 67.

You can control which data movers are used for backups and duplications when you configure NetBackup storage units.

See "Configuring a storage unit for cloud storage" on page 68.

Adding backup media servers to your cloud environment

You can add additional media servers to your cloud environment. Additional media servers can help improve backup performance. Such servers are known as *data movers*.

See "About cloud storage data movers" on page 67.

Adding additional media servers to the Cloud environment

1 In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Servers**.

2 Select the cloud storage server.

3 From the **Edit** menu, select **Change**.

4 In the **Change Storage Server** dialog box, select the **Media Servers** tab

5 Select the media server or servers that you want to enable for cloud backup. The operating system of any specified media servers must be a supported operating system. The media servers that are checked are configured as cloud servers.

6 Click **OK**.

7 Copy the appropriate configuration file from the media server that you specified when you configured the storage server. The file name depends on your storage vendor. The following is the format:

`libstspi`*`VendorName`*`.conf`

The file resides in the following directory, depending on operating system:

- UNIX and Linux: `/usr/openv/lib/ost-plugins/`
- Windows: `install_path\VERITAS\NetBackup\bin\ost-plugins\`

8 Save the file to the appropriate directory on the media server or servers that you added, as follows:

- UNIX and Linux: `/usr/openv/lib/ost-plugins/`
- Windows: `install_path\VERITAS\NetBackup\bin\ost-plugins\`

Caution: If you do not copy the `libstspi`*`VendorName`*`.conf` to the new media server, any backups that attempt to use the media server fail. The backups fail with a NetBackup Status Code 83 (media open error).

---

9 Modify disk pools, storage units, and policies as desired.

Configuring a storage unit for cloud storage

Create one or more storage units that reference the disk pool.

The **Disk Pool Configuration Wizard** lets you create a storage unit; therefore, you may have created a storage unit when you created a disk pool. To determine if storage units exist for the disk pool, see the **NetBackup Management > Storage > Storage Units** window of the Administration Console.

A storage unit inherits the properties of the disk pool. If the storage unit inherits replication properties, the properties signal to a NetBackup storage lifecycle policy the intended purpose of the storage unit and the disk pool. Auto Image Replication requires storage lifecycle policies.

You can use storage unit properties to control your backup traffic.

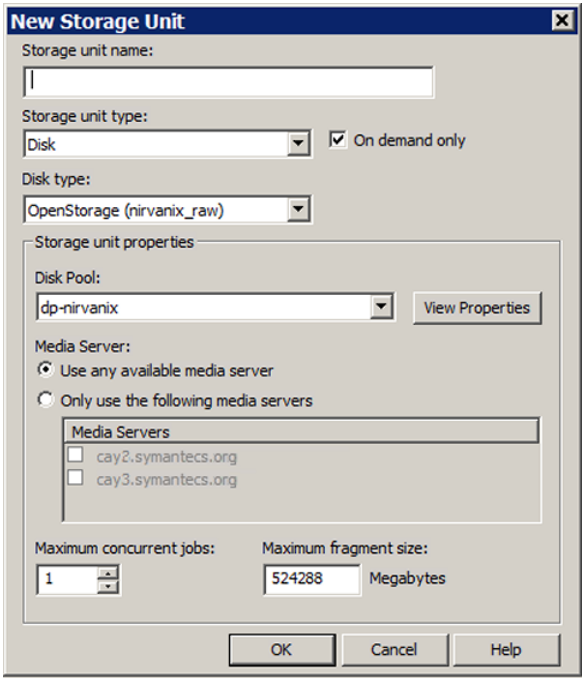
See “Configure a favorable client-to-server ratio” on page 71.

See “Control backup traffic to the media servers” on page 72.

To configure a storage unit from the Actions menu

1 In the **NetBackup Administration Console**, expand **NetBackup Management > Storage > Storage Units**.

2 On the **Actions** menu, select **New > Storage Unit**.



3 Complete the fields in the **New Storage Unit** dialog box.

See “Cloud storage unit properties” on page 69.

Cloud storage unit properties

The following are the configuration options for a cloud disk pool storage unit.

Table 2-20 Cloud storage unit properties

Property	Description
Storage unit name	A unique name for the new storage unit. The name can describe the type of storage. The storage unit name is the name used to specify a storage unit for policies and schedules. The storage unit name cannot be changed after creation.
Storage unit type	Select **Disk** as the storage unit type.
Disk type	UNIX: Select **Cloud Storage (*type*)** for the disk type. *type* represents the disk pool type, based on storage vendor, encryption, and so on. Windows: Select **OpenStorage (*type*)** for the disk type. *type* represents the disk pool type, based on storage vendor, encryption, and so on.
Disk pool	Select the disk pool that contains the storage for this storage unit. All disk pools of the specified **Disk type** appear in the **Disk pool** list. If no disk pools are configured, no disk pools appear in the list.
Media server	The **Media server** setting specifies the NetBackup media servers that can deduplicate the data for this storage unit. Only the deduplication storage server and the load balancing servers appear in the media server list. Specify the media server or servers as follows: ■ To allow any server in the media server list to deduplicate data, select **Use any available media server**. ■ To use specific media servers to deduplicate the data, select **Only use the following media servers**. Then, select the media servers to allow. NetBackup selects the media server to use when the policy runs.

Table 2-20 Cloud storage unit properties *(continued)*

Property	Description
Maximum concurrent jobs	The **Maximum concurrent jobs** setting specifies the maximum number of jobs that NetBackup can send to a disk storage unit at one time. (Default: one job. The job count can range from 0 to 256.) This setting corresponds to the Maximum concurrent write drives setting for a Media Manager storage unit. NetBackup queues jobs until the storage unit is available. If three backup jobs are scheduled and **Maximum concurrent jobs** is set to two, NetBackup starts the first two jobs and queues the third job. If a job contains multiple copies, each copy applies toward the **Maximum concurrent jobs** count. **Maximum concurrent jobs** controls the traffic for backup and duplication jobs but not restore jobs. The count applies to all servers in the storage unit, not per server. If you select multiple media servers in the storage unit and 1 for **Maximum concurrent jobs**, only one job runs at a time. The number to enter depends on the available disk space and the server's ability to run multiple backup processes. **Warning:** A Maximum concurrent jobs setting of 0 disables the storage unit.
Maximum fragment size	For normal backups, NetBackup breaks each backup image into fragments so it does not exceed the maximum file size that the file system allows. You can enter a value from 20 MBs to 51200 MBs. For a FlashBackup policy, Symantec recommends that you use the default, maximum fragment size to ensure optimal duplication performance.

Configure a favorable client-to-server ratio

You can use storage unit settings to configure a favorable client-to-server ratio. Uou can use one disk pool and configure multiple storage units to separate your backup traffic. Because all storage units use the same disk pool, you do not have to partition the storage.

For example, assume that you have 100 important clients, 500 regular clients, and four media servers. You can use two media servers to back up your most important clients and two media servers to back up your regular clients.

The following example describes how to configure a favorable client-to-server ratio:

- Configure the media servers for NetBackup deduplication and configure the storage.
- Configure a disk pool.
- Configure a storage unit for your most important clients (such as STU-GOLD). Select the disk pool. Select **Only use the following media servers**. Select two media servers to use for your important backups.
- Create a backup policy for the 100 important clients and select the STU-GOLD storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.
- Configure another storage unit (such as STU-SILVER). Select the same disk pool. Select **Only use the following media servers**. Select the other two media servers.
- Configure a backup policy for the 500 regular clients and select the STU-SILVER storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.

Backup traffic is routed to the wanted data movers by the storage unit settings.

Note: NetBackup uses storage units for media server selection for write activity (backups and duplications) only. For restores, NetBackup chooses among all media servers that can access the disk pool.

Control backup traffic to the media servers

On disk pool storage units, you can use the **Maximum concurrent jobs** settings to control the backup traffic to the media servers. Effectively, this setting directs higher loads to specific media servers when you use multiple storage units for the same disk pool. A higher number of concurrent jobs means that the disk can be busier than if the number is lower.

For example, two storage units use the same set of media servers. One of the storage units (STU-GOLD) has a higher **Maximum concurrent jobs** setting than the other (STU-SILVER). More client backups occur for the storage unit with the higher **Maximum concurrent jobs** setting.

About NetBackup Accelerator and NetBackup Optimized Synthetic backups

NetBackup Cloud Storage supports NetBackup Accelerator and NetBackup Optimized Synthetics. Encryption, metering, and throttling are functional and

supported when you enable NetBackup Accelerator or NetBackup Optimized Synthetic backups. You enable both NetBackup Accelerator and NetBackup Optimized Synthetic backups in the same way as non-Cloud backups. More information about NetBackup Accelerator and NetBackup Optimized Synthetic backups is available.

- Symantec NetBackup Deduplication Guide UNIX, Windows, Linux
- Symantec NetBackup Administrator's Guide, Volume I

Enabling NetBackup Accelerator with cloud storage

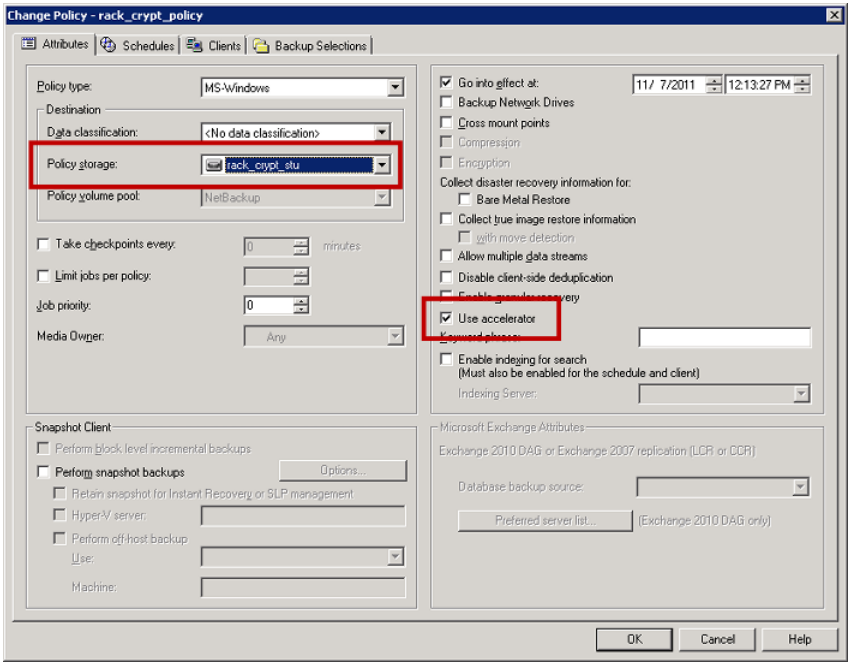
Use the following procedure to enable NetBackup Accelerator for use with NetBackup cloud storage.

Enabling Accelerator for use with NetBackup cloud storage

1. In the NetBackup Administration Console, select **NetBackup Management > Policies > *policy_name***. Select **Edit > Change**, and select the **Attributes** tab.
2. Select **Use accelerator**.
3. Confirm the **Policy storage** option is a valid Cloud storage unit.

   The storage unit that is specified under **Policy storage** must be one of the supported Cloud vendors. You can't set **Policy storage** to **Any Available**.

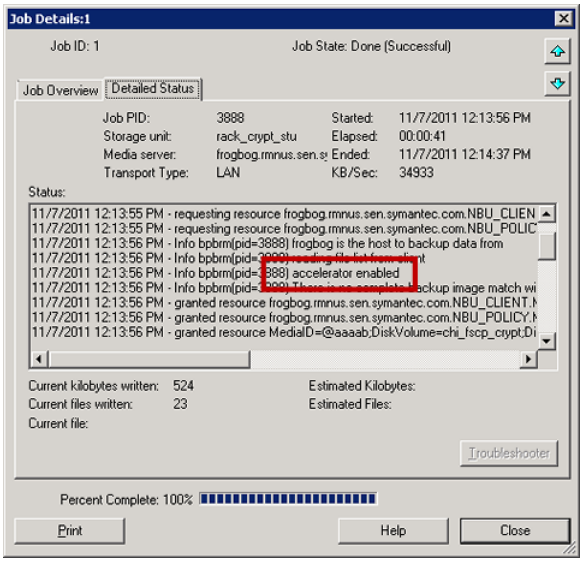
Figure 2-2 Enable Accelerator



Determining if NetBackup Accelerator was used during a backup operation

1. In the NetBackup Administration Console, select **Activity Monitor**. Double click the backup that you want to check.
2. Click the **Detailed Status** tab.
3. Review the status for **accelerator enabled**. This text indicates the backup used NetBackup Accelerator.

Figure 2-3 Confirm Accelerator used during backup



Enabling optimized synthetic backups with cloud storage

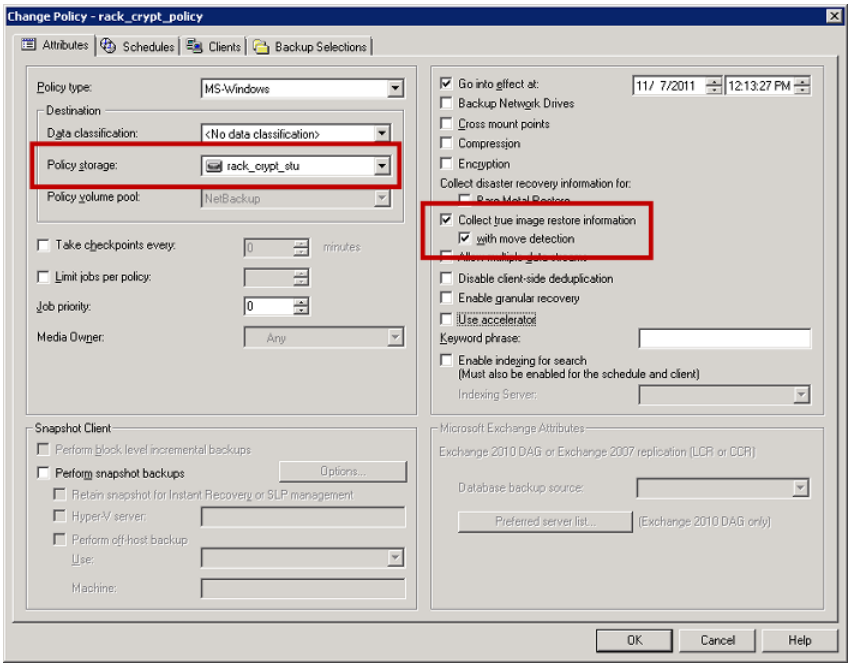
Optimized Synthetic backups require three backup schedules. You must have a **Full backup**, an **Incremental backup**, and a **Full Backup with Synthetic backup enabled**. You can use either a Differential incremental or a Cumulative incremental for the incremental backup. You must then perform a full backup, then at least one incremental backup, and finally a full backup with synthetic enabled. The final backup is the optimized synthetic backup.

Enabling Optimized Synthetic backups for use with NetBackup Cloud Storage

1. In the NetBackup Administration Console, select **NetBackup Management > Policies > *policy_name***. Select **Edit > Change**, and select the **Attributes** tab.
2. Select **Collect true image restore information** and **with move detection**.
3. Confirm the **Policy storage** option is a valid Cloud storage unit.

   The storage unit that is specified under **Policy storage** must be one of the supported Cloud vendors. You can't set **Policy storage** to **Any Available**.

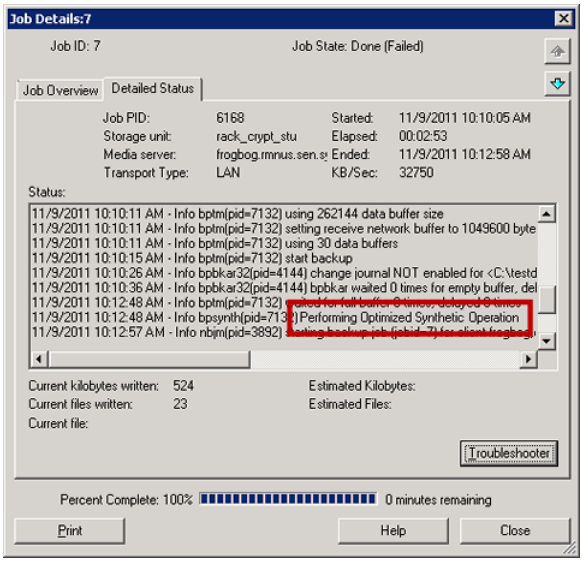
Figure 2-4 Enable Optimized Synthetic backups



Determining if a backup was an Optimized Synthetic backup

1. In the NetBackup Administration Console, select **Activity Monitor**. Double click the backup that you want to check.
2. Click the **Detailed Status** tab.
3. Review the status for **Performing Optimized Synthetic Operation**. This text indicates the backup was an Optimized Synthetic backup.

Figure 2-5 Confirm backup was Optimized Synthetic



Creating a backup policy

The easiest method to set up a backup policy is to use the **Policy Configuration Wizard**. This wizard guides you through the setup process by automatically choosing the best values for most configurations.

Not all policy configuration options are presented through the wizard. For example, calendar-based scheduling and the **Data Classification** setting. After the policy is created, modify the policy in the **Policies** utility to configure the options that are not part of the wizard.

Note: Do not use the Policy Configuration Wizard to configure policies for Replication Director.

Using the Policy Configuration Wizard to create a backup policy

Use the following procedure to create a backup policy with the Policy Configuration Wizard.

To create a backup policy with the Policy Configuration Wizard

1. In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.
2. In the right pane, click **Create a Policy** to begin the **Policy Configuration Wizard**.
3. Select **File systems, databases, applications**.
4. Click **Next** to start the wizard and follow the prompts.

Click **Help** on any wizard panel for assistance while running the wizard.

Creating a backup policy without using the Policy Configuration Wizard

Use the following procedure to create a backup policy in the **NetBackup Administration Console** without using the Policy Configuration Wizard.

To create a policy without the Policy Configuration Wizard

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
2. On the **Actions** menu, click **New > Policy**.
3. Type a unique name for the new policy in the **Add a New Policy** dialog box.
4. If necessary, clear the **Use Policy Configuration Wizard** checkbox.
5. Click **OK**.
6. Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

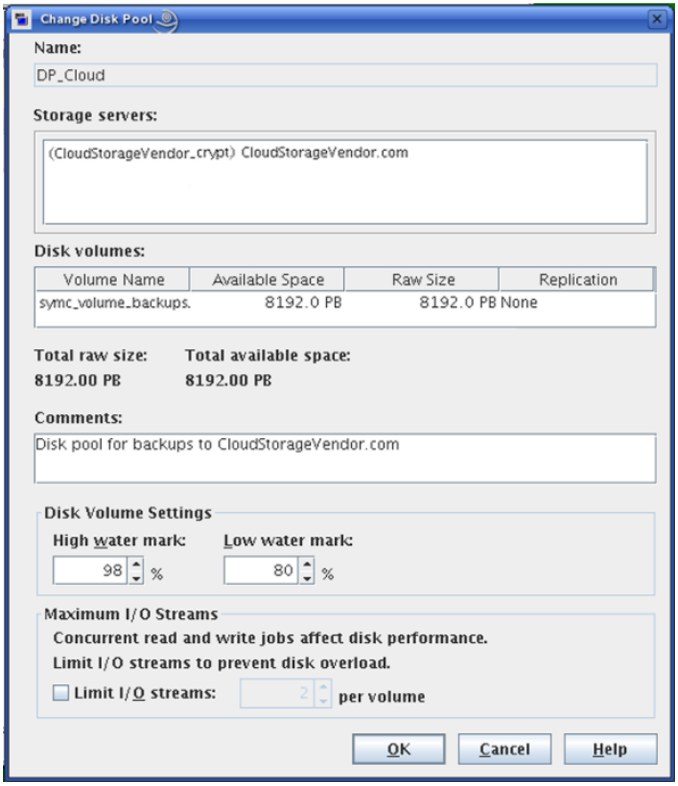
Changing cloud storage disk pool properties

You can change some of the properties of a disk pool.

To change disk pool properties

1. In the NetBackup Administration Console, expand **Media and Device Management > Devices > Disk Pools**.
2. Select the disk pool that you want to change in the details pane.

3 On the **Edit** menu, select **Change**.



4 Change the properties as necessary.

See “Cloud storage disk pool properties” on page 79.

5 Click **OK**.

Cloud storage disk pool properties

The properties of an disk pool may vary depending on the purpose the disk pool. The following table describes the possible properties:

Table 2-21 Cloud storage disk pool properties

Property	Description
Name	The disk pool name.
Storage server	The storage server name.

Table 2-21 Cloud storage disk pool properties *(continued)*

Property	Description
Disk volumes	The disk volume that comprises the disk pool.
Total size	The total amount of space available in the disk pool.
Total raw size	The total raw, unformatted size of the storage in the disk pool. The storage host may or may not expose the raw size of the storage.
Comment	A comment that is associated with the disk pool.
High water mark	The **High water mark** setting is a threshold that triggers the following actions: ■ When an individual volume in the disk pool reaches the **High water mark**, NetBackup considers the volume full. NetBackupchooses a different volume in the disk pool to write backup images to. ■ When all volumes in the disk pool reach the **High water mark**, the disk pool is considered full. NetBackup fails any backup jobs that are assigned to a storage unit in which the disk pool is full. NetBackup also does not assign new jobs to a storage unit in which the disk pool is full. ■ NetBackup begins image cleanup when a volume reaches the **High water mark**; image cleanup expires the images that are no longer valid. For a disk pool that is full, NetBackup again assigns jobs to the storage unit when image cleanup reduces any disk volume's capacity to less than the **High water mark**. The default is 98%.
Low water mark	The **Low water mark** is a threshold at which NetBackup stops image cleanup. The**Low water mark** setting cannot be greater than or equal to the **High water mark** setting. The default is 80%.
Limit I/O streams	Select to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit. When the limit is reached, NetBackup chooses another volume for write operations, if available. If not available, NetBackup queues jobs until a volume is available. Too many streams may degrade performance because of disk thrashing. Disk thrashing is excessive swapping of data between RAM and a hard disk drive. Fewer streams can improve throughput, which may increase the number of jobs that complete in a specific time period. A starting point is to divide the **Maximum concurrent jobs** of all of the storage units by the number of volumes in the disk pool.

Table 2-21 Cloud storage disk pool properties *(continued)*

Property	Description
per volume	Select or enter the number of read and write streams to allow per volume. Many factors affect the optimal number of streams. Factors include but are not limited to disk speed, CPU speed, and the amount of memory. For the disk pools that are configured for **Snapshot** and that have a **Replication source** property: ■ Always use increments of 2 when you change this setting. A single replication job uses two I/O streams. ■ If more replication jobs exist than streams are available, NetBackup queues the jobs until streams are available. ■ Batching can cause many replications to occur within a single NetBackup job. Another setting affects snapshot replication job batching.

Chapter 3

Monitoring and Reporting

This chapter includes the following topics:

Viewing cloud storage job details

Use the NetBackup Activity Monitor to view job details.

To view cloud storage job details

1. In the **NetBackup Administration Console**, click **Activity Monitor**.
2. Click the **Jobs** tab.
3. To view the details for a specific job, double-click on the job that is displayed in the **Jobs** tab pane.
4. In the **Job Details** dialog box, click the **Detailed Status** tab.

Reporting and monitoring cloud backups

All monitoring and reporting for NetBackup Cloud is handled through NetBackup OpsCenter. Please refer to the NetBackup OpsCenter Administrator's Guide for details on cloud monitoring and reporting.

Reporting on Auto Image Replication jobs

The Activity Monitor displays both the **Replication** job and the **Import** job in a configuration that replicates to a target master server domain.

Table 3-1 Auto Image Replication jobs in the Activity Monitor

Job type	Description
Replication	The job that replicates a backup image to a target master displays in the Activity Monitor as a **Replication** job. The **Target Master** label displays in the **Storage Unit** column for this type of job. Similar to other **Replication** jobs, the job that replicates images to a target master can work on multiple backup images in one instance. The detailed status for this job contains a list of the backup IDs that were replicated.
Import	The job that imports a backup copy into the target master domain displays in the Activity Monitor as an **Import** job. An **Import** job can import multiple copies in one instance. The detailed status for an **Import** job contains a list of processed backup IDs and a list of failed backup IDs. **Note:** If the master servers in the source and target domains are not at the same NetBackup version, the following error can occur under certain circumstances: Failed to auto create data classification. This error occurs if the master server in the source domain is at a NetBackup version earlier than 7.6 and the data classification of **Any** is used. If the master server in the target domain is at NetBackup 7.6, use a different data classification in the source domain or the Import job fails. Note that a successful replication does not confirm that the image was imported at the target master. If the data classifications are not the same in both domains, the **Import** job fails and NetBackup does not attempt to import the image again. Failed **Import** jobs fail with a status 191 and appear in the **Problems** report when run on the target master server. The image is expired and deleted during an **Image Cleanup** job. Note that the originating domain (Domain 1) does not track failed imports.

Displaying KMS key information for cloud storage encryption

You can use the `nbkmsutil` command to list the following information about the key groups and the key records:

- Key groups. See To display KMS key group information.
- Keys. See To display KMS key information.

Note: Symantec recommends that you keep a record key information. The key tag that is listed in the output is necessary if you need to recover keys.

The following are the directories in which the `nbkmsutil` command resides:

- UNIX: `/usr/openv/netbackup/bin/admincmd`
- Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd`

To display KMS key group information

- To list all of the key groups, use the `nbkmsutil` with the `-listkgs` option. The following is an example:

```
nbkmsutil -listkgs

Key Group Name        : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : -
```

To display KMS key information

- To list all of the keys that belong to a key group name, use the `nbkmsutil` with the `-listkgs` and `-kgname` options. The following is an example:

```
nbkmsutil -listkeys -kgname CloudStorageVendor.com:symc_volume_for_backup

Key Group Name        : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : -

  Key Tag      : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
  Key Name              : Encrypt_Key_April
  Current State         : Active
  Creation Time         : Tues Jan 01 01:02:00 2013
  Last Modification Time: Tues Jan 01 01:02:00 2013
  Description           : -
```

Chapter 4

Troubleshooting

This chapter includes the following topics:

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. Unified logging creates log file names and messages in a standardized format. All NetBackup processes use either unified logging or legacy logging.

Unlike the files that are written in legacy logging, unified logging files cannot be viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file.

See “About legacy logging” on page 88.

Server processes and client processes use unified logging.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\NetBackup\logs`

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using the following commands:

`vxlogcfg`	Modifies the unified logging configuration settings. for more information about the `vxlogcfg` command.
`vxlogmgr`	Manages the log files that the products that support unified logging generate. for more information about the `vxlogmgr` command.
`vxlogview`	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 87. for more information about the `vxlogview` command.

See the NetBackup Commands Reference Guide for a complete description about these commands.

These commands are located in the following directory:

UNIX	`/usr/openv/netbackup/bin`
Windows	*`install_path`*`\NetBackup\bin`

About using the vxlogview command to view unified logs

Use the `vxlogview` command to view the logs that unified logging creates. These logs are stored in the following directory.

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\logs`

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

You can use `vxlogview` to view NetBackup log files as well as PBX log files.

To view PBX logs using the `vxlogview` command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.
- To specify the PBX product ID. enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Table 4-1 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/05 06:51:48 AM" -e "05/03/05 06:52:48 AM"`

Table 4-1 Example uses of the vxlogview command *(continued)*

Item	Example
Display results faster	You can use the `-i` option to specify an originator for a process: `# vxlogview -i nbpem` The `vxlogview -i` option searches only the log files that the specified process (`nbpem`) creates. By limiting the log files that it has to search, `vxlogview` returns a result faster. By comparison, the `vxlogview -o` option searches all unified log files for the messages that the specified process has logged. **Note:** If you use the `-i` option with a process that is not a service, `vxlogview` returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the `-o` option instead of the `-i` option. The -i option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).
Search for a job ID	You can search the logs for a particular job ID: `# vxlogview -i nbpem | grep "jobid=`*`job_ID`*`"` The `jobid=` search key should contain no spaces and must be lowercase. When searching for a job ID, you can use any `vxlogview` command option. This example uses the `-i` option with the name of the process (`nbpem`). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the jobid=*job_ID*.

A complete description of `vxlogview` is in the NetBackup Commands Reference Guide.

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. In legacy debug logging, each process creates logs of debug activity in its own logging directory. All NetBackup processes use either unified logging or legacy logging.

See "About unified logging" on page 85.

To enable legacy debug logging on NetBackup servers, you must first create the appropriate directories for each process.

UNIX	`/usr/openv/netbackup/logs` `/usr/openv/volmgr/debug`
Windows	*`install_path`*`\NetBackup\logs` *`install_path`*`\Volmgr\debug`

After the directories are created, NetBackup creates log files in the directory that is associated with each process. A debug log file is created when the process begins.

To enable debug logging for the NetBackup Status Collection Daemon (`vmscd`), create the following directory before you start `nbemm`.

As an alternative, you can stop and restart `nbemm` after creating the following directory:

UNIX	`/usr/openv/volmgr/debug/reqlib`
Windows	*`install_path`*`\Volmgr\debug\reqlib\`

Tables are available that list the log directories that you must create.

Note: On a Windows server, you can create the debug log directories at once, under *`install_path`*`\NetBackup\Logs`, by running the following batch file: *`install_path`*`\NetBackup\Logs\mklogdir.bat`.

Media servers have only the `bpbrm`, `bpcd`, `bpdm`, and `bptm` debug logs.

Creating NetBackup log file directories

Before you configure a feature that uses the OpenStorage framework, create the directories into which NetBackup commands write log files. Create the directories on the master server and on each media server that you use for OpenStorage. The log files reside in the following directories:

- UNIX: `/usr/openv/netbackup/logs/`
- Windows:*`install_path`*`\NetBackup\logs\`

More information about NetBackup logging is available.

See the *NetBackup Troubleshooting Guide*.

See "About NetBackup cloud storage log files" on page 90.

To create log directories for NetBackup commands

- Depending on the operating system, run one of the following scripts:

  UNIX: `/usr/openv/netbackup/logs/mklogdir`

  Windows: *`install_path`*`\NetBackup\logs\mklogdir.bat`

To create the `tpconfig` command log directory

- Depending on the operating system, create the `debug` directory and the `tpcommand` directory (by default, the `debug` directory and the `tpcommand` directory do not exist). The pathnames of the directories are as follows:

  UNIX: `/usr/openv/volmgr/debug/tpcommand`

  Windows: *`install_path`*`\Veritas\Volmgr\debug\tpcommand`

About NetBackup cloud storage log files

NetBackup cloud storage exists within the Symantec OpenStorage framework. Therefore, the log files for cloud activity are the same as for OpenStorage with several additions.

Some NetBackup commands or processes write messages to their own log files. For those commands and processes, the log directories must exist so that the utility can write log messages.

See "Creating NetBackup log file directories" on page 89.

Other processes use Veritas unified log (VxUL) files. Each process has a corresponding VxUL originator IDs. VxUL uses a standardized name and file format for log files. To view VxUL log files, you must use the NetBackup `vxlogview` command.

More information about how to view and manage VxUL log files is available.

See the NetBackup Troubleshooting Guide.

The following are the component identifiers for log messages:

- An `sts_` prefix relates to the interaction with the plug-in that writes to and reads from the storage.
- A cloud storage server prefix relates to interaction with that cloud vendor's storage network.
- An `encrypt` prefix relates to interaction with the encryption plug-in.
- A `KMSCLIB` prefix relates to interaction with the NetBackup Key Management Service.

Most interaction occurs on the NetBackup media servers. Therefore, the log files on the media servers that you use for disk operations are of most interest.

Warning: The higher the log level, the greater the affect on NetBackup performance. Use a log level of 5 (the highest) only when directed to do so by a Symantec representative. A log level of 5 is for troubleshooting only.

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup master server. The log levels for some processes specific to certain options are set in configuration files as described in Table 4-2.

Table 4-2 describes the logs.

Table 4-2 NetBackup logs

Activity	OID	Processes
Backups and restores	N/A	Messages appear in the log files for the following processes: ■ The `bpbrm` backup and restore manager. ■ The `bpdbm` database manager. ■ The `bpdm` disk manager. ■ The `bptm` tape manager for I/O operations. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/` ■ Windows: *`install_path`*`\NetBackup\logs\`
Backups and restores	117	The `nbjm` Job Manager.
Image cleanup, verification, import, and duplication	N/A	The `bpdbm` database manager log files. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/bpdbm` ■ Windows: *`install_path`*`\NetBackup\logs\bpdbm`
Cloud connection operations	N/A	The `bpstsinfo` utility writes information about connections to the cloud storage server in its log files.
Cloud account configuration	222	The the Remote Manager and Monitor Service is the process that creates the cloud storage accounts. RMMS runs on media servers.
Cloud Storage Service Container	N/A	The NetBackup Cloud Storage Service Container (`nbcssc`) writes log files to the following directories: ■ For Windows: *`install_path`*`\NetBackup\logs\nbcssc` ■ For UNIX/Linux: `/usr/openv/netbackup/logs/nbcssc`

Table 4-2 NetBackup logs *(continued)*

Activity	OID	Processes
Credentials configuration	N/A	The `tpconfig` utility. The `tpconfig` command writes log files to the `tpcommand` directory.
Device configuration	111	The `nbemm` process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration	202	The Storage Server Interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

Enable libcurl logging

Set the storage server property *`CLOUD_PREFIX`*`:LOG_CURL` to `YES` to enable cURL logging. The `CLOUD_PREFIX` value is the prefix value of each storage provider. The possible values are:

- AMZ for Amazon
- ATT for AT&T
- RACKS for Rackspace

To example, to enable `LOG_CURL` for AT&T set `ATT:LOG_CURL` to `YES`.

See "Changing storage server properties in NetBackup" on page 65.

NetBackup CloudStore Service Container startup and shutdown troubleshooting

Do not change the security mode of the NetBackup CloudStore Service Container while the service is active. If the security mode is changed while the service is active, you may encounter service startup or service shutdown problems.

More information is available if the NetBackup CloudStore Service Container service does not start.

See "Connection to the NetBackup CloudStore Service Container fails" on page 93.

If the NetBackup CloudStore Service Container fails during service shutdown, check the `CSSC_IS_SECURE` attribute. You can find this value in the CloudStore configuration file for UNIX or Linux or the registry for Windows. Determine if the `CSSC_IS_SECURE` attribute is the same as the current mode of the service. Be sure to stop the service in the same mode it was started.

See "Stopping and starting the NetBackup CloudStore Service Container" on page 93.

Connection to the NetBackup CloudStore Service Container fails

The `csconfig` command makes three attempts to connect to the NetBackup CloudStore Service Container with a 60-second timeout for each connection attempt. If the connection attempt fails, verify the following information:

- Make sure that your firewall settings are appropriate or firewall is disabled.
- Check the security mode as defined by the `CSSC_IS_SECURE` attribute in the CloudStore configuration file (for UNIX or Linux) or the registry (for Windows). The current mode should be same as that when the Service was started.
- If the `CSSC_IS_SECURE` value equals `1` and the service fails to start, the server certificate may be corrupt or expired. Review the cssc log file for error messages similar to the following (bold added for emphasis):

  `[1326119109] [error] [client unknown host] set_ssl_option:` **`cannot open C:\Program Files\Veritas\NetBackup\bin\ost-plugins\cssc.crt:`** `error:0906D064 EM routines EM_read_bio:bad base64 decode.`

  One of the causes of this error message is a corrupt or an expired server certificate file. The server certificate file is `cssc.crt`. It is in the `/usr/openv/lib/ost-plugins` directory on UNIX or Linux and *`install_path`*`\Veritas\Netbackup\bin\ost-plugins` on Windows. To recreate this file, delete the file and restart the service.

  More information about the cssc log file is available.

  See "About the NetBackup CloudStore Service Container" on page 27.

See "Stopping and starting the NetBackup CloudStore Service Container" on page 93.

Stopping and starting the NetBackup CloudStore Service Container

Use the **NetBackup Administration Console** to stop and start the NetBackup CloudStore Service Container (`nbcssc`) service.

See "About the NetBackup CloudStore Service Container" on page 27.

To start or stop the CloudStore Service Container

1. In the **NetBackup Administration Console**, expand **NetBackup Administration > Activity Monitor**.
2. Click the **Daemons** tab (UNIX or the **Services** tab (Windows).
3. In the **Details** pane, select **nbcssc** (UNIX and Linux) or **NetBackup CloudStore Service Container** Windows).
4. On the **Actions** menu, select **Stop Selected** or **Start Selected** (Windows) or **Stop Daemon** or **Start Daemon** (UNIX).

Troubleshooting cloud storage configuration issues

The following sections may help you troubleshoot configuration issues.

Cannot create a cloud storage disk pool

The following table describes potential solutions if you cannot create a disk pool in NetBackup.

Table 4-3 Cannot create disk pool solutions

Error	Description
`The wizard is not able to obtain Storage Server information. Cannot connect on socket. (25)`	The error message appears in the **Disk Configuration Wizard**. The **Disk Configuration Wizard** query to the cloud vendor host timed-out. The network may be slow or a large number of objects (for example, buckets on Amazon S3) may exist. To resolve the issue, use the NetBackup `nbdevconfig` command to configure the disk pool. Unlike the wizard, the `nbdevconfig` command does not monitor the command response times. See "Configuring a disk pool for cloud storage" on page 56.

Troubleshooting cloud storage operational issues

The following sections may help you troubleshoot operational issues.

See "Cloud storage backups fail with status code 84 or 87" on page 95.

See "A restart of the nbcssc process reverts all cloudstore.conf settings" on page 96.

See "NetBackup Administration Console fails to open" on page 97.

Cloud storage backups fail with status code 84 or 87

The following topics describe the backup failures that can result in status code 84 or 87 in the NetBackup job details.

Accelerator backups fail

A message similar to the following is in the job details:

```
Critical bptm(pid=28291) accelerator verification failed: backupid=
  host_name_1373526632, offset=3584, length=141976576, error=
  2060022, error message: software error
Critical bptm(pid=28291) image write failed: error 2060022: software
  error
Error bptm(pid=28291) cannot write image to disk, Invalid argument end
  writing; write time: 0:02:31
Info bptm(pid=28291) EXITING with status 84
Info bpbkar(pid=6044) done. status: 84: media write error media write
  error(84)
```

This error may occur in the environments that have more than one cloud storage server. It indicates that NetBackup Accelerator backups of a client to one cloud storage server were later directed to a different cloud storage server.

For Accelerator backups to cloud storage, ensure the following:

- Always back up each client to the same storage server. Do so even if the other storage server represents storage from the same cloud storage vendor.
- Always use the same backup policy to back up a client, and do not change the storage destination of that policy.

Backups fail after the WRITE_BUFFER_SIZE is increased

If the cloud storage server `WRITE_BUFFER_SIZE` property exceeds the total swap space of the computer, backups can fail with a status 84.

Adjust the `WRITE_BUFFER_SIZE` size to a value lower than the computer's total swap space to resolve this issue.

The cloud vendor interface created the volume

A message similar to the following is in the job details:

```
Info bptm(pid=xxx) start backup
Critical bptm(pid=xxxx) image open failed: error 2060029: authorization
  failure
Error bpbrm(pid=xxxx) from client gabby: ERR - Cannot write to STDOUT. E
```

```
  rrno  = 32: Broken pipe
Info bptm(pid=xxxx) EXITING with status 84
```

A message similar to the following appears in the `bptm` log file:

```
Container container_name is not Symantec container or tag data error,
fail to create image. Please make sure that the LSU is created by
means of NBU.
```

This error indicates that the volume was created by using the cloud storage vendor's interface.

You must use the NetBackup **Disk Pool Configuration Wizard** to create the volume on the cloud storage. The wizard applies a required partner ID to the volume. If you use the vendor interface to create the container, the partner ID is not applied.

To resolve the problem, use the cloud storage vendor's interface to delete the container. In NetBackup, delete the disk pool and then recreate it by using the **Disk Pool Configuration Wizard**.

See "Viewing cloud storage job details" on page 82.

See "About NetBackup cloud storage log files" on page 90.

AIX media server backs up large files

When an AIX media server backs up large files, you may encounter memory issues. These memory issues can result in failed backups. The backups fail with a NetBackup status code 84 (media write error) or a NetBackup status code 87 (media close error). Change the AIX `ulimit` size to unlimited to resolve this issue. Be sure to stop and restart the NetBackup services or daemons after you change the `ulimit` value.

The following are examples:

```
ulimit -m unlimited
```

```
ulimit -d unlimited
```

```
ulimit -s unlimited
```

A restart of the nbcssc process reverts all cloudstore.conf settings

Missing entries and comments are not allowed in the `cloudstore.conf` file. If you remove or comment out values in the `cloudstore.conf` file, a restart of the `nbcssc` process returns all settings to their default values.

NetBackup Administration Console fails to open

If you change the default port of the NetBackup CloudStore Service Container, the **NetBackup Administration Console** may not open. You must change the value in two places.

The CloudStore Service Container configuration file	The CloudStore Service Container configuration file resides in the following directories: ■ Windows: *install_path*\Veritas\NetBackup\bin\cloudstorewin.conf ■ UNIX: /usr/openv/java/cloudstorejava.conf The following is an example that shows the default value: [NBCSSC] NBCSSC_PORT=5637
The operating system's services file	The services file is in the following locations: ■ Windows: C:\WINDOWS\system32\drivers\etc\services ■ Linux: /etc/services

If you change the value in the CloudStore Service Container configuration file also change the value in the services file.

By default, the NetBackup CloudStore Server Container port is 5637.

Chapter 5

Known issues

This chapter includes the following topics:

About using the bpstsinfo to list storage server information

When using the `bpstsinfo` command to list storage server information, use either the `-stype` option or the `-storageserverprefix` option. If you do not use one of these two options, the command attempts to find the storage server name in all providers. This action frequently takes too long to complete and causes the command to fail.

Encrypted and non-encrypted storage units displayed in bpstsinfo command output

When using the `bpstsinfo` command to display the encrypted logical storage unit (LSU) information, the output shows both encrypted and non-encrypted LSUs.

Example:

```
bpstsinfo -lsuinfo -storage_server amazon.com -stype amazon_crypt
```

Displaying both encrypted and non-encrypted LSUs is an expected result. The `bpstsinfo` command operates on the level of the storage plug-in which is not aware of any higher level detail, such as encryption. As such, when you use the `bpstsinfo` command with the `-lsuinfo` operation, all potential LSUs on that level are returned, regardless of their use within NetBackup.

About inconsistencies when image information is displayed

Due to the nature of the cloud plugins, each plugin returns image information on the basis of its own interpretation of the image. When using commands to list image properties, be aware the plugin that requested the information affects the information that is returned. When using the `bpstsinfo` command to list images, specify the same option for `-stype` that was used at the time of backup.

Deleting NetBackup cloud storage servers

If you incorrectly remove a storage server, configuration files are left orphaned on the computer. Attempts to create a new storage server fail with an error message that indicates a login failure. Use the following procedure to correctly delete a storage server:

Deleting a storage server

1. Expire all images on the storage server.
2. Delete the storage unit.
3. Delete the disk pool.
4. Delete the storage server.
5. Delete the `.conf` and `.pref` files from `lib/ost-plugins` or `bin/ost-plugins` directory.

Special characters and the csconfig command

Do not specify a directory with special characters when issuing the `csconfig meter -directory` command. The operating system's shell may incorrectly interpret the directory path which leads to unexpected results.

Directory length exceeds maximum path length for csconfig command

The `csconfig meter -directory dir` command sets the metering directory path and creates the directory if it does not exist. The directory creation fails if directory value exceeds the maximum path length limit for the system or if there are permission issues. If the directory creation fails, NetBackup uses the default directory. The default directory is `/usr/openv/netbackup/bin/ost-plugins` for UNIX and Linux. The default directory is *install_path*`\NetBackup\bin` for Windows.

Unexpected results for csconfig throttle command

Do not use `cloud_global` as the `stype` when you set the maximum connections with the `csconfig throttle` command. This term is a reserved keyword and can lead to unexpected results. The `stype` value should be one of the acceptable values that is listed in the Throttling options and their values table.

Different cloud provider information provided to the csconfig throttle command

When setting the maximum connections using `csconfig throttle` command, make sure the cloud provider for the `stype` and the `sserver` are the same. If you provide two different providers, the provider name that is passed with the `sserver` command is used.

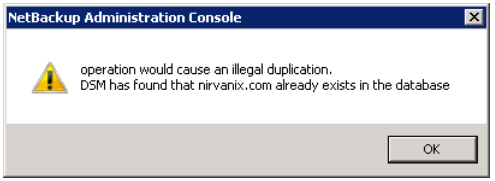
Attempts to set available bandwidth with the csconfig command fail

The `csconfig throttle` command accepts large values for the available bandwidth option. The maximum allowed value varies with the operating system where the

NetBackup CloudStore Service Container resides. Refer to the `csconfig` log file if the command fails.

Unable to configure additional media servers

If you attempt to run the Cloud wizard on a second media server that uses the same master server as the first media server, you receive an `illegal duplication` error.



Your only options in the wizard are to click **Cancel** or **Back**. If you click **Back**, there are no configuration changes that allow the wizard to continue.

You must use the correct procedure if you want multiple media servers in your Cloud environment. More information is available on this topic.

See "Adding additional media servers to the Cloud environment" on page 67.

Cloud configuration may fail if NetBackup Access Control is enabled

When you attempt to configure Cloud in an environment that uses NetBackup Access Control, you may receive an error. The error is `Error creating Key Group and Keyscannot connect on socket`. This error is generated because the user trying to configure Cloud does not have sufficient rights within NetBackup Access Control. The user account that configures Cloud must be a member of the NBU_KMS Admin Group if you use NetBackup Access Control. See the NetBackup Security and Encryption Guide for more information on NetBackup Access Control and account setup.

Index

S

U

V

W